SOME CONTRIBUTIONS TO DIOPHANTINE EQUATIONS

A Thesis Submitted
in Partial Fulfilment of the Requirements
for the Degree of
DOCTOR OF PHILOSOPHY

By
AYYADURAI MEENAKSHI SUNDARA RAMASAMY

to the

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY KANPUR

OCTOBER 1982

SOME CONTRIBUTIONS TO DIOPHANTINE EQUATIONS

A Thesis Submitted
in Partial Fulfilment of the Requirements
for the Degree of
DOCTOR OF PHILOSOPHY

By
AYYADURAI MEENAKSHI SUNDARA RAMASAMY

to the

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY KANPUR

OCTOBER 1982

11/10/83

CERTIFICATE

This is to certify that the work embodied in the thesis 'SOME CONTRIBUTIONS TO DIOPHANTINE EQUATIONS' by Ayyadurai Meenakshi Sundara Ramasamy has been carried out under my supervision and has not been submitted elsewhere for a degree or diploma.

October, 1982.

[S.P.Mohanty]
Professor
Department of Mathematics,
Indian Institute of Technology,
Kanpur.

Dedicated

to the sacred memory of

my beloved father

Sri D.R. Ayyadurai Ayer

CONTENTS

ACKNOWLEDGMENT

I have immense pleasure to express my deep sense of gratitude, sincerest appreciation and profound regards to my beloved teacher Professor Dr. S.P.Mohanty, a guiding star in teaching and research, for his all-time encouragement, continuous inspiration, thought-provoking lectures, illuminating discussions, excellent guidance, affection and wishes ; for having aroused my interest in Number theory ; and for having given me more of his time than I had any right to take. I thank the Almighty for having offered me a golden opportunity to be a student of my distinguished guide.

I sincerely thank the University Grants Commission for having offered me a teacher fellowship under the Faculty Improvement Programme, without which I could not have done my research work. I am very much indebted to the Indian Institute of Technology,Kanpur, for having provided me with all modern facilities congenial for research. I am sincerely thankful to the Mathematics Department, Central Library, Computer Centre and the Graphic Arts for the help rendered to me.

I express my profound gratitude to Prof.R.Balasubramanian, Principal, A.V.C. College, Mannampandal, Mayiladuthurai, for his encouragement and help to undertake this research work. I am greatly indebted to the Chairman, Secretary and Correspondent and the

for having granted me study leave from July,1979 to October, 1982. I am extremely thankful to my colleagues Professors D.Antony Durairaj, A.Rajamohan, N.Ramanathan and N.Seshadri for all their help. I am deeply grateful to Prof.P.S.Sankaran of Pope's College, Sawyerpuram for his generous help and blessings. I sincerely thank my friends Messers.K.S.Arulsamy, N.Bhavani Shankar Rao, Govinda Raj and D.Madhava Rao for their help.

I wish to express my thanks to my affectionate wife Girija for her patient help during the years of my research.

Finally I thank Messers. Ashok Kumar Bhatia, G.L.Misra and S.K.Tewari for their typing and Mr. A.N.Upadyaya for cyclostyling the thesis.

A.M.S. Ramasamy

October,1982. (A.M.S.RAMASAMY)

SYNOPSIS

Of 'SOME CONTRIBUTIONS TO DIOPHANTINE EQUATIONS' , a thesis submitted in partial fulfilment of the requirements for the Ph.D. degree by Ayyadurai Meenakshi Sundara Ramasamy to the Department of Mathematics, Indian Institute of Technology, Kanpur.

Organization of the thesis : This thesis consists of 5 chapters. We give chapterwise references. The following are numbered chapterwise : (i) Lemmas, Theorems and Corollaries, (ii) Tables, (iii) Remarks and (iv) Equations.

In our Diophantine equations the unknowns are supposed to be rational integers. By an integral solution of a Diophantine equation, we mean a rational integral solution.

S.P. Mohanty gave a method to obtain all the integral solutions of the Diophantine equation

$$x^3 + y + 1 - xyz = 0$$

and W.R. Utz determined all the positive integral solutions of the Diophantine equation

$$x^3 + 2y + 1 - xyz = 0.$$

In Chapter 1 we give a method for obtaining all the positive ntegral solutions of the Diophantine equation

$$ax^3 + by + c - xyz = 0$$

here a,b,c are given positive integers, c is square-free and d (ab,c) = 1. Further we give some polynomial solutions

without any restriction on a,b and c. We also consider the cases when (i) $c = 1$ and (ii) $a = c = 1$, in view of the fact that the computations can be simplified considerably in these special cases. We prove that the number of positive integral solutions of the Diophantine equation

$$x^3 + by + 1 - xyz = 0 \ (b > 0)$$

is odd when b is a prime $\neq 3$ and even for $b = 3$ and give a conjecture on the number of positive integral solutions of this equation. At the end of the chapter we give tables of solutions in some particular cases.

Let N be any given non-zero integer. A method to obtain all the solutions in non-zero integers of the Diophantine equation

$$(x^2 + y)(x + y^2) = N(x-y)^3$$

was given by R.J. Stroeker. In Chapter 2 we generalise his method and show how to secure all the solutions of the Diophantine equation

$$(x^2 + by)(bx + y^2) = N(x-y)^3$$

in non-zero integers where b is any given positive integer. For $b = N$, we give some polynomial solutions. Given b, we show that there are infinitely many values of N for which the equation under consideration has at least five non-zero integral solutions. We give tables of solutions for the cases

(i) $1 \leq N \leq 100$ and $1 \leq b \leq 4$ and (ii) $1 \leq N \leq 10$ and $5 \leq b \leq 10$. In an appendix we provide a computer program using which all but a few of the integral solutions can be obtained for given b and N.

In Part I of Chapter 3 we consider the Pell's equations $A^2-DB^2 = 1$ and $U^2 - DV^2 = N$ where D is any given square-free natural number and N is any given non-zero integer. We give some relations for the solutions (when they exist) of the equation $U^2 - DV^2 = N$. We define the characteristic numbers of the systems

$$\text{(i)} \quad \left.\begin{aligned} U^2 - DV^2 &= N \\ Z^2 - gU^2 &= h \end{aligned}\right\}$$

$$\text{(ii)} \quad \left.\begin{aligned} U^2 - DV^2 &= N \\ Z^2 - gV^2 &= h \end{aligned}\right\}$$

where g,h are given integers. In Part II of Chapter 3 we consider some applications of Pell's equation. We indicate that the functions η_r and ξ_r, introduced by Tharmambikai Ponnudurai in one of her previous papers, can be dispensed with and her Diophantine problem can be handled quite easily by our relations. We generalize a theorem of A.Brauer and prove that the system of simultaneous Diophantine equations

$$\left.\begin{aligned} x^2 + x + 1 &= 3z^i \\ y^2 + y + 1 &= 3z^j \end{aligned}\right\}$$

has no integral solutions except $z = 1$, where i and j are different positive integers. Based on the work of some authors, we give the following

DEFINITION : Let k be a given positive integer. Two integers α and β are said to have the property p_k (resp. p_{-k}) if $\alpha\beta + k$ (resp. $\alpha\beta - k$) is a perfect square.

The following results are established : There is no other positive integer ρ which shares the property

(i) p_{-1} with 2,5, and 13

(ii) p_{-1} with 5,13 and 34

(iii) p_{-1} with 1,5,and 10

(iv) p_4 with 1,5,12 and 96.

We also discuss the simultaneous Diophantine equations

$$\left.\begin{aligned} 2x^2 - 1 &= y^2 \\ 6x^2 - 5 &= z^2 \end{aligned}\right\},$$

arising from the three numbers 2,4 and 12 which share the property p_1.

In Chapter 4 we define a P_k set and a $P_{r,k}$ sequence. We provide a construction for a $P_{3,k}$ sequence. It is shown that the sequence so constructed is related to the Fibonacci numbers $\{F_n\}$. We derive the relation

$$F_{2n}^2+F_{2n+2}^2+F_{2n+4}^2-2F_{2n}F_{2n+2}-2F_{2n+2}F_{2n+4}-2F_{2n}F_{2n+4} = 4.$$

We define an F-type $P_{3,k}$ sequence and exhibit its relationship with a sequence of Fibonacci type. We show how the terms of an F-type $P_{3,k}$ sequence and the solutions of the Diophantine equation

$$x^2 - 5y^2 = 4k$$

are inter-connected. We prove that the number of distinct classes of solutions of this equation is divisible by 3 and as a consequence we find the invalidity of a statement of B. Stolt. We also discuss the Diophantine equation

$$X^2 + 33Y^2 = Z^2.$$

Finally the following theorem is proved : If $k \equiv 2 \pmod 4$, then there is no $P_{r,k}$ sequence with $r \geq 4$.

Let $N'(k)$ denote the number of coprime integral solutions x,y of the Mordell's equation

$$y^2 = x^3 + k.$$

S.P. Mohanty has proved that $\limsup_{k \to \infty} N'(k) \geq 6$ and N.M.Stepens has proved that $\limsup_{k \to \infty} N'(k) \geq 8$. In Chapter 5 we prove that $\limsup_{k \to \infty} N'(k) \geq 12$. Denoting the number of coprime integer solutions of the Diophantine equation

$$y^2 = ax^3 + k$$

by $N'(a,k)$, Jingcheng Tong proved that $\limsup_{k \to \infty} N'(a,k) \geq 6$ holds for odd integer a and raised the following

PROBLEM. Does $\limsup_{k \to \infty} N'(a,k) \geq 6$ hold for even integer a?

We prove that the answer to his question is in the affirmative. In fact we prove the result for the more general Diophantine equation

$$by^2 = ax^3 + k$$

where a and b are any given non-zero integers. Finally, in Tong's notation, we prove the following theorem :

$$\limsup_{k \to \infty} N'(4,k) \geq 8.$$

CHAPTER 1

THE DIOPHANTINE EQUATION $ax^3+by+c-xyz = 0$

1. INTRODUCTION

According to W.H.Mills [5], ''In spite of the efforts of many mathematicians of the last 300 years, comparatively few general methods of solving non-linear Diophantine equations are available, and much of the literature on the subject consists of isolated results. When it comes to systems of simultaneous non-linear Diophantine equations, the results become even more fragmentary, and a complete solution of such a system is a rarity''. He has studied the system $x \mid y^2+ay+1$, $y \mid x^2+ax+1$, where a is a fixed integer. Many interesting results have been obtained for the equation $z = f_1(x,y) \mid f_2(x,y)$ when $f_1(x,y)$ and $f_2(x,y)$ are special quadratic polynomials. These are due to E.S. Barnes [1], K.Goldberg, M. Newman, E.G.Straus and J.D.Swift [2], W.H.Mills [5], A.Schinzel and W.Sierpinski [10] and T.N.Sinha [11] . We also refer to L.J.Mordell [9] for a system of Diophantine equations. For the equation $x^3 + y + 1 -xyz = 0$, S.P. Mohanty [7] has given all 9 positive integral solutions and in [8] he has obtained all integral solutions of this equation. For the equation $x^3 + 2y + 1 -xyz = 0$, W.R.Utz [12] has given all 13 positive integral solutions.

Our aim in this chapter is to provide a method for obtaining all the positive integral solutions of the

Diophantine equation

$$ax^3 + by + c - xyz = 0 \tag{1}$$

where a,b,c are given positive integers, c is square-free and $\gcd(ab,c) = 1$.

2. SOME POLYNOMIAL SOLUTIONS

First we give some polynomial solutions for (1) where a,b,c are given positive integers without any restriction. One can easily check that (1) is always satisfied by any one of the following positive triads :

$$\left.\begin{array}{l}(x,y,z) = (1,1,a+b+c),(1,a+c,b+1),\\ (b+c,1,ab^2+ac^2+2abc+1),\\ (b+1,ab^3+3ab^2+3ab+a+c,1),\\ (abc^2+b+c,ac^2+1,a^2b^2c^2+ab^2+2abc+1),\\ (ab^3+b+c,a^3b^6+3a^2b^4+2a^2b^3c+3ab^2+ac^2+3abc+1,1),\\ (a^2b^3c^2+2ab^2c+b+c,a^3b^3c^3+3a^2b^2c^2+ac^2+3abc+1,a^2b^3c+ab^2+1).\end{array}\right\} \tag{2}$$

3. METHOD OF SOLVING THE TITLE EQUATION

Let (x,y,z) be a positive integral solution of (1). Clearly $x = 1$ implies $y \mid a+c$ and $(x,y,z) = (1,\frac{a+c}{t},b+t)$ where t is a positive divisor of a+c. Hereafter we always consider $x > 1$.

Throughout the rest of this section we assume that c is square-free and $\gcd(ab,c) = 1$. The following lemma,

the proof of which is easy, is useful for the computation of the positive integral solutions of (1).

LEMMA 1.1. Let (x,y,z) be a positive integral solution of (1). Then we have

(i) $\gcd(b,x) = 1$, (ii) $\gcd(a,y) = 1$ and

(iii) $\gcd(c,x) = 1 \iff \gcd(c,y) = 1$.

If (x,y,z) is a positive integral solution of (1) with $\gcd(c,x) = g \neq 1$, then $g \mid y$. Write $c = gc_1$, $x = gx_1$ and $y = gy_1$. Then (1) is transformed into

$$ag^2x_1^3 + by_1 + c_1 - gx_1y_1z = 0.$$

Putting $ag^2 = A$, $b = B$, $c_1 = C$, $x_1 = X$, $y_1 = Y$ and $gz = Z$, we have the equation

$$AX^3 + BY + C - XYZ = 0.$$

It is not difficult to check that C is square-free, $\gcd(AB,C) = 1$ and $\gcd(C,X) = 1$. Consequently it follows that whenever (x,y,z) is a positive integral solution of (1), we can assume without loss of generality that $\gcd(c,x) = 1$.

Following [7,8], the problem of solving (1) in positive integers x,y,z is transformed into an equivalent problem as provided by

LEMMA 1.2. (x,y,z) is a positive integral solution of (1) with $\gcd(c,x) = 1$ if and only if (x,y) is a positive integral

solution of the system

$$x \mid by + c, \; y \mid ax^3 + c$$

with $\gcd(c,xy) = 1$.

Proof. Let (x,y,z) be a positive integral solution of (1) with $\gcd(c,x) = 1$. Then clearly $\gcd(c,xy) = 1$, $x \mid by+c$ and $y \mid ax^3+c$.

Conversely, let (x,y) be a positive integral solution of the system

$$x \mid by + c, \; y \mid ax^3 + c$$

with $\gcd(c,xy) = 1$. Then $xy \mid (ax^3+c)(by+c)$, or $xy \mid c(ax^3+by+c)$. Since $\gcd(c,xy) = 1$, we have $xy \mid ax^3+by+c$. Hence there exists a positive integer z such that $ax^3+by+c-xyz = 0$.

Therefore, to solve (1) in positive integers (x,y,z) with $\gcd(c,x) = 1$, we consider the equivalent system $x \mid by+c$ and $y \mid ax^3+c$ with $\gcd(c,xy) = 1$ and follow the method of attack as in [7,8].

Let x,y be positive integers such that $x \mid by+c$, $y \mid ax^3+c$ and $\gcd(c,xy) = 1$. Then there are two positive integers r,s such that

$$rx = by + c \qquad (3)$$

and

$$sy = ax^3 + c. \qquad (4)$$

When $r = c = 1$, we have $x = by+1$. Hence $y \mid ax^3+1$ implies $y \mid a(by+1)^3+1$, and so $y \mid a+1$. Let v be a positive divisor of $a+1$. Denote $\frac{a+1}{v}$ by u. We then have $(x,y,z) = (bu+1, u, ab^2u+2ab+v)$. When $c > 1$, from (3) it follows that $\gcd(c,r) = 1$. Next, we have an observation for the pair (r,x). If $(r,x)=(c+1,2)$, then (3) implies $by = c+2$. Let v_1 be a positive divisor of $c+2$ and take $u_1 = \frac{c+2}{v_1}$. Choosing $b = u_1$ and $y = v_1$, we have $z = \frac{ax^3+by+c}{xy} = \frac{8a+bv_1+c}{2v_1}$. For those positive integers v_1 satisfying $2v_1 \mid 8a+bv_1+c$, we have $(x,y,z) = (2, v_1, \frac{8a+bv_1+c}{2v_1})$. Hereafter we will not consider the pairs $(r,c) = (1,1)$ and $(r,x) = (c+1,2)$. Using our assumption that $\gcd(ab,c) = 1$ we conclude from (3) that $\gcd(b,r) = 1$. This fact is useful while we compute the solutions of (1). From (4) we have $\gcd(c,s) = 1$ and $\gcd(s,x) = 1$.

Elimination of y from (3) and (4) yields

$$x(sr-abx^2) = c(s+b). \qquad (5)$$

(5) implies $sr > abx^2$ and $c \mid x(sr-abx^2)$. Since $\gcd(c,x) = 1$, we have $c \mid sr-abx^2$. Hence $\frac{sr-abx^2}{c}$ is a positive integer. Write

$$n = \frac{sr-abx^2}{c}. \qquad (6)$$

We then have from (5),

$$nx = s+b. \qquad (7)$$

From (6) and (7) we have

$$abx^2 = sr-cn = (nx-b)r - cn,$$

or,

$$br+cn = x(nr-abx). \tag{8}$$

(8) forces $nr > abx$. So there exists a positive integer k such that

$$nr = abx+k. \tag{9}$$

From (8) and (9) we have

$$kx = br+cn \tag{10}$$

and finally

$$(n-b)(r-c) + (k-ab)(x-1) = b(a+c). \tag{11}$$

From (9) and (10) we conclude that

$$b \mid n \iff b \mid k. \tag{12}$$

We write

$$A = (n-b)(r-c),$$

$$B = (k-ab)(x-1)$$

so that (11) becomes

$$A+B = b(a+c). \tag{13}$$

LEMMA 1.3. The following statements are equivalent :

(i) The system

$$\left.\begin{aligned} &x \mid by+c \\ &y \mid ax^3+c \\ &\gcd(c,xy) = 1 \end{aligned}\right\} \qquad (I)$$

is solvable in positive integers x,y.

(ii) The system

$$\left.\begin{aligned} &sy = ax^3+c \\ &s \equiv -b \pmod{x} \\ &\gcd(c,xy) = 1 \end{aligned}\right\} \qquad (II)$$

is solvable in positive integers x,y,s.

(iii) There exist positive integers x,n such that

$$y = \frac{ax^3+c}{nx-b} \quad \text{and } \gcd(c,xy) = 1.$$

(iv) The system

$$\left.\begin{aligned} &sy = ax^3+c \\ &by = rx-c \\ &s = nx-b \\ &\gcd(c,xy) = 1 \end{aligned}\right\} \qquad (III)$$

is solvable in positive integers x,y,n,r,s .

(v) The system

$$\left.\begin{aligned} A+B &= b(a+c) \\ nr &= abx+k \\ by &= rx-c \\ \gcd(c,xy) &= 1 \end{aligned}\right\} \qquad (IV)$$

is solvable in positive integers k,n,r,x,y.

(vi) The system

$$\left.\begin{aligned} A+B &= b(a+c) \\ kx &= br+cn \\ by &= rx-c \\ \gcd(c,xy) &= 1 \end{aligned}\right\} \qquad (V)$$

is solvable in positive integers k,n,r,x,y,

Proof. From our preceding discussion, it is clear that (i) implies (ii), (iii), (iv), (v) and (vi).

(ii) ==> (i). Assume (ii) holds. Then $y \mid ax^3+c$. From $sy = ax^3+c$ and $s \equiv -b \pmod x$, we obtain $-by \equiv c \pmod x$.

(iii) ==> (ii). Take $s = nx-b$.

(iv) ==> (i). Clear.

One can easily check that (v) ==> (vi) ==> (v).

(v) ==> (i). Assume (v) holds. From $nr = abx+k$, we have $rx = \dfrac{abx^2+kx}{n}$. Using $kx = br+cn$, we get $rx - c = \dfrac{b(ax^2+r)}{n}$. Because of $by = rx-c$, it follows that $ny = ax^2+r$. Using this we obtain $ax^3+by+c = x(ny-r)$

Now, in order to find the solutions of the system (IV), we have to consider the cases $(A,B) = (+,+),(+,-)$, $(-,+),(b(a+c),0)$, $(0,b(a+c))$, to exhaust all the possibilities. The second one does not occur for $a = b = 1$ and the third one does not occur for $b = c = 1$.

Before discussing the method of obtaining all the positive integral solutions of (1), we prove some theorems. The first one is very important in that it considerably simplifies the working.

THEOREM 1.4. (x,y,z) is a positive integral solution of (1) with $\gcd(c,x) = 1$ if and only if

$$z = n \tag{14}$$

where n is given by (6).

Proof. Since $ax^3+by+c-xyn = ax^3+by+c-xy(\frac{sr-abx^2}{c})$ (using (6))

$$= \frac{1}{c}(acx^3+bcy+c^2-(rx)(sy)+abx^3y)$$

$$= 0 \text{(using (3), (4))},$$

(x,y,n) satisfies (1).

Conversely, if (x,y,z) is a positive integral solution of (1) with $\gcd(c,x) = 1$, clearly $z = n$. This establishes the theorem.

THEOREM 1.5. Let $x = x_1, y = y_1, z = z_1$ be a positive integral solution of (1) with $s = s_1$ such that $x_1 \mid b^2-c$. Then $x = x_1, y = s_1, z = z_2$ is a positive integral solution of (1) with $s = y_1$ where z_2 is a positive integer.

Proof. We have $z_1 = \dfrac{ax_1^3+by_1+c}{x_1y_1}$ and $s_1y_1 = ax_1^3 + c$. Let $z_2 = \dfrac{ax_1^3+bs_1+c}{x_1s_1}$. Then $z_2 = \dfrac{s_1y_1+bs_1}{x_1s_1} = \dfrac{y_1+b}{x_1}$. Since $x_1 | by_1+c$ and $x_1 | b^2-c = b(y_1+b)-(by_1+c)$, we have $x_1 | b(y_1+b)$. But $\gcd(b,x_1) = 1$. Therefore $z_2 = \dfrac{y_1+b}{x_1}$ is an integer.

COROLLARY 1.6. When $x | b^2-c$, x appears an even number of times as a solution of (1) unless $s = y$ for the corresponding value of x.

When $s = y$, from (4) we have

$$y^2 = ax^3+c. \tag{15}$$

Multiplying both sides of (15) by a^2, we obtain a Mordell's equation

$$Y^2 = X^3+M \tag{16}$$

where $X = ax$, $Y = ay$, $M = a^2c$. It is well known that given a positive integer M, (16) has only a finite number of integral solutions. The solutions of (16) for various values of M have been obtained by O. Hemer [3], M.Lal, M.F.Jones and B.J.Blundon [4] and S.P.Mohanty [6]. From the solutions of (16), we consider those solutions satisfying $X,Y > 0$ and $X,Y \equiv 0 \pmod a$, to secure positive integral solutions of (15).

THEOREM 1.7. Let $x = x_1$, $y = y_1$, $z = z_1$ be a positive integral solution of (1) with $r = r_1$ such that $y_1 | a^2c^2-c$. Then

$x = r_1$, $y = y_1$, $z = z_2$ is a positive integral solution of (1) with $r = x_1$.

Proof. Consider $\dfrac{ar_1^3+by_1+c}{r_1y_1} = \dfrac{a(by_1+c)^2+x_1^3}{x_1^2y_1}$.

Let $N = a(by_1+c)^2+x_1^3$. Since $by_1+c \equiv 0 \pmod{x_1}$, we have $N \equiv 0 \pmod{x_1^2}$. Again $N \equiv x_1^3+ac^2 \pmod{y_1} \equiv ax_1^3+a^2c^2 \pmod{y_1}$. Since $a^2c^2 \equiv c \pmod{y_1}$, we obtain $N \equiv ax_1^3+c \pmod{y_1} \equiv 0 \pmod{y_1}$ Because $\gcd(x_1,y_1) = 1$, it follows that $\dfrac{N}{x_1^2y_1}$ is an integer. We take $\dfrac{N}{x_1^2y_1} = z_2$.

COROLLARY 1.8. When $y \mid a^2c^2-c$, y appears an even number of times as a solution of (1) unless $r = x$ for the corresponding value of $\bar{y}$.

THEOREM 1.9. A necessary and sufficient condition for $x = r$ to yield a positive integral solution of (1) is that there exist two positive integers t,w such that

$$4ct^2 + 4abct + b^2 = w^2,\ 2t \mid b+w \text{ and } 2t^2 \mid 2act + b + w.$$

Proof. Assume $x = r$ yields a positive integral solution of (1). Using $x = r$ in (3) we obtain

$$x^2 = by + c. \tag{17}$$

(9) with $r = x$, $n = z$ gives

$$xz = abx + k. \tag{18}$$

(18) implies $x \mid k$. So $\frac{k}{x}$ is a positive integer. Let $\frac{k}{x} = t$.

Using $k = tx$ in (18) we obtain

$$z = ab + t.$$

Using this in (10) with $r = x$, $k = tx$ and $n = z$, we have the quadratic equation

$$tx^2 - bx - c(ab+t) = 0. \tag{19}$$

Solving for x, we get

$$x = \frac{b \pm \sqrt{4ct^2+4abct+b^2}}{2t}.$$

Obviously, $-$ sign cannot hold. In order that x is an integer, we must have

$$4ct^2+4abct+b^2 = w^2 \tag{20}$$

for some positive integer w. So $x = \frac{b+w}{2t}$. This implies $2t \mid b+w$. Now from (17) we obtain $y = \frac{x^2-c}{b} = \frac{2act+b+w}{2t^2}$ (using (20)). Thus $2t^2 \mid 2act+b+w$. This proves the necessity of the condition.

Next assume that t, w are positive integers with the stated properties. Then consider

$$(x,y,z) = \left(\frac{b+w}{2t}, \frac{2act+b+w}{2t^2}, ab+t \right).$$

We have $ax^3+by+c-xyz$

$$= \frac{1}{8t^3}\left[a(b+w)^3+4abt(2act+b+w)+8ct^3-2(b+w)(2act+b+w)(ab+t)\right]$$

$$= \frac{1}{8t^3}\left[(b+w)\{a(b+w)^2-2(b+w)(ab+t)-4act(ab+t)+4bt\} + 8abct^2+8ct^3\right]$$

$$= \frac{1}{8t^3}\,[(b+w)(2bt-2tw)+8abct^2+8ct^3]$$

$$= \frac{1}{4t^2}\,(b^2-w^2+4abct+4ct^2) = 0,$$

proving that (x,y,z) is a positive integral solution of (1) with $x = r$.

THEOREM 1.10. Let $x = x_1$, $y = y_1$, $z = z_1$ be a positive integral solution of (1) with $s = s_1$ such that $s_1 \mid b^3-1$. Then $x = z_1$, $y = y_2$, $z = x_1$ is a positive integral solution of

$$cx^3+by+a-xyz = 0$$

with $s = s_1$, where y_2 is a positive integer.

Proof. From (1) we have $y_1 = \dfrac{ax_1^3+c}{x_1z_1-b}$ and from (7), $x_1z_1=s_1+b$. We must prove that $\dfrac{cz_1^3+a}{z_1x_1-b}$ is an integer. This expression

$$= \frac{c\left(\frac{s_1+b}{x_1}\right)^3+a}{s_1} = \frac{ax_1^3+c(s_1+b)^3}{s_1x_1^3}.$$

(7) implies $x_1 \mid s_1+b$. So $x_1^3 \mid ax_1^3+c(s_1+b)^3$. From (4), s_1 satisfies $s_1 \mid ax_1^3+c$ and $\gcd(c,s_1) = 1$. Since $c(b^3-1) = ax_1^3+cb^3-(ax_1^3+c)$ and $s_1 \mid b^3-1$, we have $s_1 \mid ax_1^3+c(s_1+b)^3$. Since $\gcd(s_1,x_1) = 1$, it follows that $\dfrac{cz_1^3+a}{z_1x_1-b}$ is an integers.

Now we return to the method of obtaining the positive integral solutions of (1) in the various cases.

Case (I). $(A,B) = (+,+)$. This case gives $b(a+c)-1$ subcases. The ith subcase $(1 \leq i \leq ab+bc-1)$ is $(A,B) = (i, ab+bc-i)$. Hence

$$(r-c)(z-b) = i$$

and

$$(k-ab)(x-1) = ab+bc-i.$$

So

$$r-c \mid i, z-b \mid i, k-ab \mid ab+bc-i \text{ and } x-1 \mid ab+bc-i.$$

In view of Lemma 1.3., we take those solutions (k,r,x,z) of (13) in the ith subcase of Case (I), which also satisfy (9) and $rx \equiv c \pmod b$. Further we confine ourselves to those r's and x's satisfying $\gcd(b,r) = 1$, $\gcd(b,x) = 1$, $(r,x) \neq (c+1,2)$. Having known r and x, we can find y using $y = \frac{rx-c}{b}$.

Case (II). $(A,B) = (+,-)$. In this case k can take one of the values $1,2,\ldots, ab-1$. Elimination of n from (9) and (10) yields

$$(kr-abc)x = br^2+ck. \qquad (21)$$

(21) implies $kr > abc$ and

$$br^2+ck \equiv 0 \pmod{kr-abc}.$$

Letting $b_1 = \frac{b}{\gcd(b,k)}$, $k_1 = \frac{k}{\gcd(b,k)}$, we have

$$b_1r^2 + ck_1 \equiv 0 \pmod{k_1r-ab_1c}.$$

Therefore

$$a^2b_1^3c^2+ck_1^3 = -b_1(k_1r+ab_1c)(k_1r-ab_1c)+k_1^2(b_1r^2+ck_1)$$
$$\equiv 0 \pmod{k_1r-ab_1c}.$$

Thus

$$kr-abc \;\Big|\; \frac{a^2b^3c^2 + ck^3}{(\gcd(b,k))^2}. \tag{22}$$

We factorise $\frac{a^2b^3c^2+ck^3}{(\gcd(b,k))^2}$ and select those factors which are $\equiv -abc \pmod k$. These give the values of r. For given k and r, we have in Case (II).

$$x = \frac{br^2+ck}{kr-abc}.$$

From (3), $y = \frac{rx-c}{b}$; substituting for x from the above, we get

$$y = \frac{ac^2+r^3}{kr-abc} \tag{23}$$

using which we can evaluate y. In order to obtain integral values of y, we restrict to those pairs (r,x) satisfying $rx \equiv c \pmod b$. z can be determined from $z = \frac{kx-br}{c}$ (see (10)), which, when substituted for x, gives

$$z = \frac{ab^2r+k^2}{kr-abc}. \tag{24}$$

Case (III). $(A,B) = (-,+)$. This gives two subcases: Case (III(i)): $z = 1,2,..,b-1$ and $r > c$, Case (III(ii)): $r = 1,2,...,c-1$ and $z > b$. Case (III(ii)) does not occur if c=1

Case (III(i)). Fix z. Eliminating r from (9) and (10), we obtain

$$(kz-ab^2)x = bk+cz^2. \qquad (25)$$

(25) implies $kz > ab^2$. We have

$$xz = b + \frac{ab^3+cz^3}{kz-ab^2} \qquad (26)$$

and hence $kz-ab^2 \mid ab^3+cz^3$. We factorise ab^3+cz^3 and choose those factors which are $\equiv -ab^2 \pmod z$. These give the values of k. For given z and k, we have in Case III(i)

$$x = \frac{bk+cz^2}{kz-ab^2}.$$

Having known x and z, we can find y using $y = \dfrac{ax^3+c}{xz-b}$.

Case (III(ii)). Fix r. From (21) we have

$$x = \frac{br^2+ck}{kr-abc}$$

and

$$rx = c + \frac{abc^2+br^3}{kr-abc}. \qquad (27)$$

(27) implies $kr-abc \mid abc^2+br^3$. We factorise abc^2+br^3 and select those factors which are $\equiv -abc \pmod r$. These give the values of k. We find x from $x = \dfrac{br^2+ck}{kr-abc}$, y from (23) and z from (24).

Case (IV). $(A,B) = (b(a+c),0)$. In this case $k = ab$ and hence by (12), $b \mid z$ and

$$(r-c)(z-b) = b(a+c). \qquad (28)$$

$b \mid z$ implies $z = bz_1$ for some positive integers z_1. So (28) becomes

$$(r-c)(z_1-1) = a+c.$$

Let v be a positive divisor of $a+c$ and take $u = \frac{a+c}{v}$.
Then $r-c = u$ and $z_1 - 1 = v$. i.e., $r = c+u$ and $z = b(v+1)$.
From (10),

$$x = \frac{br+cz}{k} .$$

Substituting for k, r and z, we get

$$x = \frac{u+c(v+2)}{a},$$

or

$$x = \frac{u+c(v+2)}{uv-c} . \qquad (29)$$

Thus $uv-c \mid u+c(v+2)$, whence $uv-c \leq u+c(v+2)$. This implies

$$(u-c)(v-1) \leq 4c. \qquad (30)$$

Since u and v are positive, we have the following possibilities :
(i) $u = 1,2,\ldots,c$; v is arbitrary, (ii) $v = 1$, u is arbitrary, (iii) $u = c+1, c+2,\ldots,5c$; $v = 2,3,\ldots, 4c+1$ subject to $(u-c)(v-1) \leq 4c$ and $uv-c \mid u+c(v+2)$. From (29), we have

$$ux = c + \frac{(c+u)^2}{uv-c}$$

and

$$vx = 1 + \frac{c(v+1)^2}{uv-c} .$$

Hence for (i) we have $uv-c \mid (c+u)^2$ and hence $v \leq \frac{c+(c+u)^2}{u}$ and for (ii) $u-c \mid 4c$ and so $u \leq 5c$. Thus, for (i), $a \leq (c+u)^2$ and hence $a \leq 4c^2$; for (ii) $a \leq 4c$; and for (iii) $a \leq 4c(c+2)$.
Thus we have

LEMMA 1.11. If $a > 4c(c+2)$, then (1) has no positive integral solutions under Case (IV).

From (3), $y = \frac{rx-c}{b}$. Substituting for r and x, we obtain

$$y = \frac{3c^2+3cu+c^2v+u^2}{b(uv-c)}. \tag{31}$$

(31) implies $b \mid 3c^2 + 3cu + c^2v + u^2$. Using this fact we can find a bound for b in Case (IV).

Case (V). $(A,B) = (0, b(a+c))$. In this case $z = b$ and hence by (12), $b \mid k$ and

$$(k-ab)(x-1) = b(a+c). \tag{32}$$

$b \mid k$ implies $k = bk_1$ for some positive integer k_1. So (32) becomes

$$(k_1-a)(x-1) = a+c.$$

Let v be a positive divisor of $a+c$ and let $u = \frac{a+c}{v}$. Then $x-1 = u$ and $k_1-a = v$. i.e., $k = b(a+v)$ and

$$x = u+1. \tag{33}$$

Now $y = \frac{ax^3+c}{xz-b}$. Substituting for x and z, we have

$$y = \frac{a(u^2+3u+3)+v}{b}. \tag{34}$$

(34) implies $b \mid a(u^2+3u+3)+v$.

LEMMA 1.12. If $\gcd(a,b) \neq 1$, then (1) has no positive integral solutions under Case (V).

Proof. Assume (1) has a positive integral solution in Case (V). Then $y = \frac{a(u^2+3u+3)+v}{b}$ is an integer where

$a+c = uv$. Assume $\gcd(a,b) = h \neq 1$. Write $a = ha_1$ and $b = hb_1$. Then $\dfrac{ha_1(u^2+3u+3)+v}{hb_1}$ is an integer. This implies $h \mid v$. Then $v \mid a+c$ implies $h \mid a+c$. Hence $h \mid ha_1+c$. This forces $h \mid c$. So $h \mid \gcd(a,c)$. But $\gcd(a,c) = 1$. Hence $h = 1$, contradiction.

LEMMA 1.13. If $a+c$ is a prime, $b \nmid 8a+c$, and $b \nmid a^3+2a^2c+3a^2+ac^2+3ac+3a+1$, then (1) has no positive integral solution in Case (V).

Proof. Since $a+c$ is a prime, we have either $u = 1$, $v = a+c$ or $u = a+c$, $v = 1$. In either case $b \nmid a(u^2+3u+3) + v$.

REMARK 1.1. In Section 3 we have discussed how the positive integral solutions of (1) can be obtained for any given positive integers a,b,c with c square-free and $\gcd(ab,c)=1$. In Section 4, we consider the special case of (1) with $c = 1$ and in Section 5, that with $a = c = 1$, in view of the fact that the computations can be simplified considerably in these special cases.

4. THE DIOPHANTINE EQUATION $ax^3+by+1-xyz = 0$

In this section we consider the Diophantine equation

$$ax^3 + by + 1 - xyz = 0 \qquad (35)$$

where a,b are given positive integers. Besides the polynomial solutions given in (2), the equation (35)

has the following additional polynomial solution :

$$(x,y,z) = (a^2b^4+2ab^2+b+1, a^4b^6+3a^3b^4+2a^2b^3+3a^2b^2+3ab+a+1, ab^2+1). \quad (36)$$

For (35), we consider the solutions in Case (IV). i.e., $(A,B) = (b(a+1),0)$. From (30), we have

$$(u-1)(v-1) \leq 4$$

where v is a positive divisor of $a+1$ and $u = \frac{a+1}{v}$. Hence we have the following possibilities : (i) $u = 1$, $v = 2,3,5$; (ii) $v = 1$, $u = 2,3,5$, (iii) $(u,v) = (2,2),(2,3),(3,2),(2,4),(4,2),(2,5),(3,3),(5,2)$. Using $x = \frac{u+v+2}{uv-1}$, one can check that $(u,v) = (2,3),(3,2),(2,4),(4,2)$ do not give integral x. From (31), $y = \frac{u^2+3u+v+3}{b(uv-1)}$ and so $b \mid u^2+3u+v+3$. The positive integral solutions of (35) obtained in Case (IV) are shown in Table 1. Thus we have secured the complete solution of (35) in Case (IV).

a	b	x	y	z	a	b	x	y	z
1	1	5	9	3	3	5	2	1	15
1	1	5	14	2	4	1	2	3	6
1	2	5	7	4	4	1	2	11	2
1	3	5	3	9	4	3	2	1	18
1	7	5	2	14	4	11	2	1	22
1	9	5	1	27	8	1	1	3	4
1	14	5	1	28	8	3	1	1	12
2	1	3	5	4	9	1	1	2	6
2	1	3	11	2	9	1	1	5	3
2	5	3	1	20	9	2	1	1	12
2	11	3	1	22	9	5	1	1	15
3	1	2	5	3					

Table 1

5. THE DIOPHANTINE EQUATION $x^3 + by + 1 - xyz = 0$

In this section we consider the Diophantine equation

$$x^3 + by + 1 - xyz = 0 \tag{37}$$

where b is a given positive integer. In addition to the polynomial solutions given in (2) and (36), the equation (37) has the solutions

$$\left.\begin{aligned}&(x,y,z) = (b+1,b+2,b+1),(b+1,b^2+b+1,2),\\&(2b+1,8b^2+4b+2,1),(b^2+1,b^2+b+1,b^2-b+2),\\&(4b^2+1,8b^2+4b+2,2b^2-b+1)\\&(b^2+1,b^4+b^3+3b^2+2b+2,1),\\&(b^3+b^2+2b+1,b^4+b^3+3b^2+2b+2,b^2+b+1).\end{aligned}\right\} \tag{38}$$

For (37), we make the following crucial remark, which simplifies the working to a great extent :

REMARK 1.2. If we simultaneously interchange x with r and k with z, then A and B are interchanged but the equation (11) remains invariant. The same is true for (3) also.

THEOREM 1.14. Let $x = x_1$, $y = y_1$, $z = z_1$ be a positive integral solution of (37) with $r = r_1$. Then $x = r_1$, $y = y_1$, $z = z_2$ is a positive integral solution of (37) with $r = x_1$ where z_2 is a positive integer.

Proof. Follows from Theorem 1.7.

COROLLARY 1.15. y appears an even number of times as a positive integral solution of (37) unless r = x for the corresponding value of y.

COROLLARY 1.16. The number of positive integral solutions of (37) is odd or even according as (37) has an odd or an even number of positive integral solutions with $r = x$.

THEOREM 1.17. A necessary and sufficient condition for $x = r$ to yield a positive integral solution of (37) is that there exists a positive integer t such that $t \mid b$ and $t^2 \mid 2t+b$.

Proof. Follows from Theorem 1.9. When t satisfies the stated properties, we have

$$(x,y,z) = \left(\frac{b}{t} + 1, \frac{b+2t}{t^2}, b+t \right).$$

COROLLARY 1.18. The number of positive integral solutions of (37) is odd or even according as the number of positive integers t given by Theorem 1.17 is odd or even.

THEOREM 1.19. If b is a prime and $b \neq 3$, the number of positive integral solutions of (37) is odd and for $b = 3$, the number of positive integral solutions of (37) is even.

Proof. Consider the positive integers t satisfying $t \mid b$ and $t^2 \mid 2t+b$. Since b is a prime, $t \mid b$ implies $t = 1$ or b. $t = 1$ always holds. $t \neq b$ unless $b = 1$ or 3. The theorem follows from Corollary 1.18.

Now we consider the method of obtaining the positive integral solutions of (37). First we have two lemmas.

LEMMA 1.20. When (x,y,z) is a positive integral solution of (37), we have

$$r = x \Longleftrightarrow k = z.$$

Proof. Follows from (9) and (10) (with $n = z$).

LEMMA 1.21. When (x,y,z) is a positive integral solution of (37), $r = x$ cannot occur in Cases (II)-(IV).

Proof. Follows from Lemma 1.20, by noting that $k \neq z$ in Cases (II)-(IV) for (37).

With regard to the Cases (II)-(V) for (37), in view of Remark 1.2. and Theorem 1.14, we conclude that it is enough if we consider Cases (II) and (IV) and whenever $x = x_1$, $y = y_1$, $z = z_1$ is a positive integral solution of (37) with $r = r_1$, we will also take $x = r_1$, $y = y_1$ with $r = x_1$ and find the corresponding z. We observe that z in Cases (II),(IV) are the same as k in Cases (III), (V) respectively.

Lemma 1.21. implies that Cases (II) and (III) yield the same number of positive integral solutions for (37) and so do Cases (IV) and (V). The solutions of (37) obtained in Case (V) are shown in Table 2.

b	x	y	z
1	2	9	1
1	3	14	1
2	3	7	2
3	2	3	3
7	3	2	7
9	2	1	9

Solutions of (37) in Case (I). For this case we have $(A,B) = (+,+)$. This implies $n > b$, $r > 1$, $k > b$ and $x > 1$. Because of Theorem 1.14, it is enough to consider $r \leq x$. When $r = x$, we can obtain the solutions by using Theorem 1.17. Therefore we consider $r < x$. From (7), we have $s = nx-b$. Substituting in (4), we obtain

$$y = \frac{x^3+1}{nx-b} .$$

By Remark 1.2., we can take $y = \frac{r^3+1}{kr-b}$. From (21), we have $x = \frac{br^2+1}{kr-b}$. Hence

$$ky-x = k\frac{r^3+1}{kr-b} - \frac{br^2+k}{kr-b} = r^2 .$$

Thus

$$ky = r^2 + x. \tag{39}$$

Using (3) and (39), we obtain

$$(k-b)y = 2-(r-1)(x-r-1). \tag{40}$$

Since $k > b$, $r > 1$, $x > r$, we have

$$(r-1)(x-r-1) = 0 \text{ or } 1.$$

Case (α). $(r-1)(x-r-1) = 0$.

Since $r > 1$, we have $x = r+1$. Using in (3), we get $by = r^2+r-1$. This implies y is odd. Now (40) implies $(k-b)y = 2$. Hence $y = 1$. This gives $b = r^2+r-1$. Thus, if b is of the form r^2+r-1 for some $r > 0$ then $x = r+1, y = 1$

is a solution of (37) and this is the only instance in which $x = r+1$.

Case (β). $(r-1)(x-r-1) = 1$.

Here $r = 2$ and $x = 4$. (40) implies $(k-b)y = 1$. Thus $y = 1$. Using in (3), we obtain $b = 7$.

A conjecture : Looking at the number N of positive integral solutions of (37) given in the following table

b :	1	2	3	4	5	6	7	8	9	10	11	12
N :	9	13	28	20	55	21	61	45	43	39	97	43

Table 3

we have the following

CONJECTURE : The number of positive integral solutions of (37)

$$\leq \begin{cases} 8b + 15, & \text{if } b \text{ is odd} \\ 4b + 15, & \text{if } b \text{ is even.} \end{cases}$$

6. THE DIOPHANTINE EQUATION $ax^3+y+c-xyz = 0$

In this section we consider the Diophantine equation

$$ax^3+y+c-xyz = 0 . \tag{41}$$

where a,c are given positive integers with $\gcd(a,c) = 1$ and c square-free. Besides the polynomial solutions given in (2), the equation (41) has also the solution

$$(x,y,z) = (c+1,1,ac^2+2ac+a+1). \tag{42}$$

For (41), we make the following important remark.

REMARK 1.3. If we simultaneously interchange a with c, k with r and x with z, then A and B are interchanged but the equation (11) remains invariant.

THEOREM 1.22. If $x = x_1$, $y = y_1$, $z = z_1$ is a positive integral solution of (41) with $s = s_1$, then $x = z_1$, $y = y_2$, $z = x_1$ is a positive integral solution of

$$cx^3+y+a-xyz = 0$$

with $s = s_1$, where y_2 is a positive integer.

Proof. Follows from Theorem 1.10.

7. SOLUTIONS IN PARTICULAR CASES

In this chapter we have discussed how all the positive integral solutions of (1) can be obtained for any given positive integers a,b,c with c square-free and gcd(ab,c) = 1. We already have solutions for (a,b,c) = (1,1,1) and (1,2,1) [7,8,12]. We give in Tables 4-20 the positive integral solutions of (1) for (a,b,c) = (1,3,1), (1,4,1),(1,5,1),(1,6,1),(1,7,1),(1,8,1),(1,9,1),(1,10,1), (1,11,1),(1,12,1),(2,1,1),(2,2,1),(2,3,1),(3,1,1),(3,2,1),(3,3,1) and (1,1,2).

Table 4. (a,b,c) = (1,3,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	5	4	13	2	10	13	8	31	1064	1
1	2	4	4	65	1	10	143	1	37	86	16
2	1	6	5	3	9	11	18	7	38	63	23
2	3	3	5	18	2	14	9	22	43	143	13
2	9	2	5	63	1	17	351	1	49	65	37
4	1	17	7	2	25	19	196	2	62	351	11
4	5	4	7	86	1	31	196	5	103	1064	10

Table 5. (a,b,c) = (1,4,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	6	5	6	5	11	74	2	65	146	29
1	2	5	5	21	2	17	21	14	69	5054	1
3	2	6	5	126	1	17	378	1	89	378	21
3	14	2	9	2	41	19	14	26	101	126	81
5	1	26	9	146	1	27	74	10	293	5054	17

Table 6. (a,b,c) = (1,5,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	7	7	172	1	19	490	1	103	247	43
1	2	6	8	3	22	23	9	59	107	171	67
2	1	7	8	19	4	23	78	7	109	305	39
2	3	4	8	27	3	23	676	1	123	172	88
2	9	3	8	171	1	26	31	22	129	490	34
3	1	11	11	2	61	26	837	1	131	17842	1
3	4	4	11	222	1	27	259	3	147	676	32
3	7	3	12	7	21	38	91	16	161	837	31
3	28	2	12	19	8	47	28	79	179	2470	13
6	1	37	12	91	2	47	2472	1	181	217	151
6	7	6	12	247	1	48	259	9	263	2472	28
6	31	2	14	305	1	68	4991	1	367	4991	27
6	217	1	17	27	11	69	2470	2	681	17842	26
7	4	13	17	78	4	101	222	46			

Table 7. (a,b,c) = (1,6,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	8	7	43	2	31	532	2	265	1634	43
1	2	7	7	344	1	37	43	32	295	344	253
5	9	4	11	9	14	37	1634	1	1375	51104	37
5	14	3	13	2	85	103	532	20			
7	1	50	13	314	1	145	314	67			
7	8	7	17	14	21	223	51104	1			

Table 8. (a,b,c) = (1,7,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	9	8	57	2	32	9	114	179	16340	2
1	2	8	8	513	1	33	14	78	179	33345	1
2	1	8	9	5	17	50	57	44	197	422	92
2	3	5	9	365	1	50	2907	1	212	333	135
2	9	4	10	7	15	54	77	38	230	2037	26
3	2	7	10	77	2	59	42	83	284	365	221
3	14	3	11	3	41	62	2037	2	351	125708	1
4	1	18	11	36	4	64	1417	3	407	2907	57
4	5	5	11	333	1	69	266	18	449	513	313
4	13	3	15	2	113	75	182	31	639	16340	25
4	65	2	15	422	1	93	9353	1	704	9353	53
5	2	14	17	182	2	95	312	29	1304	33345	51
5	7	5	23	13	41	95	1832	5	2507	125708	50
5	42	2	23	36	15	114	65	200			
8	1	65	23	312	2	135	1832	10			
8	9	8	27	266	3	155	1417	17			

Table 9. (a,b,c) = (1,8,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	10	9	730	1	35	1588	1	293	2527	34
1	2	9	11	4	31	59	140	25	307	1036	91
3	1	12	11	37	4	65	73	58	323	444	235
3	4	5	11	444	1	65	4818	1	363	1588	83
3	7	4	17	2	145	69	2527	2	521	275674	1
3	28	3	17	189	2	75	28	201	593	4818	73
5	3	10	17	546	1	89	189	42	649	730	577
5	18	3	19	7	52	101	63	162	1499	33540	67
5	63	2	19	140	3	129	3370	5	4233	275674	65
9	1	82	27	37	20	179	33540	1			
9	10	9	27	1036	1	209	3370	13			
9	73	2	29	18	47	257	546	121			

Table 10. (a,b,c) = (1,9,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	11	10	11	10	29	45	19	373	70414	2
1	2	10	10	91	2	38	21	69	374	143325	1
2	1	9	10	1001	1	38	819	2	545	666	446
2	3	6	11	6	21	41	9	187	739	552854	1
2	9	5	11	666	1	62	117	33	829	7553	91
5	1	27	14	3	66	82	91	74	901	1001	811
5	2	1	14	45	5	82	7553	1	1481	25506	86
5	6	6	14	549	1	155	25506	1	1699	70414	41
5	21	3	17	117	3	227	126	409	3449	143325	83
5	126	2	19	2	181	325	686	154	6733	552854	82
	1	101	19	686	1	353	549	227			

Table 11 (a,b,c) = (1,10,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	12	17	39	8	87	8522	1	407	936	177
1	2	11	17	702	1	101	111	92	413	702	243
3	2	8	21	2	221	101	11322	1	681	8921	52
3	14	4	21	842	1	123	86	176	983	8552	113
7	2	26	23	39	14	131	8921	2	1011	1032332	1
7	86	2	23	338	2	147	338	64	1121	11322	111
11	1	122	23	936	1	153	25046	1	1211	1332	1101
11	12	11	47	14	158	179	1235	26	1637	25046	107
11	111	2	47	1236	2	263	1236	56	10211	1032332	101
11	1332	1	69	1235	4	401	842	191			

Table 12. (a,b,c) = (1,11,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	13	14	5	40	48	2989	1	489	889	269
1	2	12	14	61	4	50	9	278	514	1355	195
2	1	10	14	915	1	56	117	27	530	819	343
2	3	7	15	4	57	57	31	105	619	844	454
2	9	6	15	844	1	57	1798	2	675	2884	158
3	1	13	17	3	97	59	252	14	675	229684	2
3	4	6	17	54	6	75	1159	5	677	465899	1
3	7	5	17	819	1	80	189	34	685	2989	157
3	28	4	20	9	45	85	8299	1	719	915	565
4	1	19	20	889	1	103	28	379	857	17919	41
4	5	6	23	2	265	119	3624	4	930	1099	787
4	13	4	23	117	5	122	133	112	1074	8299	139
4	65	3	23	1014	1	122	16359	1	1343	1818544	1
5	9	5	26	7	97	147	481	45	1475	16359	133
5	14	4	26	189	4	159	27160	1	1585	1729	1453
6	1	38	27	76	10	170	1159	25	1879	27160	130
6	7	7	29	1355	1	179	65	493	2690	56979	127
6	31	3	31	14	69	230	17919	3	3743	229684	61
6	217	2	31	76	13	233	56979	1	3909	122245	125
12	1	145	35	54	23	335	3624	31	5129	212154	124
12	13	12	36	13	100	344	122245	1	7570	465899	123
12	133	2	36	481	3	347	1798	67	14895	1818544	122
12	1729	1	47	252	9	398	217	730			
13	7	25	47	2884	1	455	212154	1			
13	1099	1	48	61	38	485	1014	232			

Table 13. (a,b,c) = (1,12,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	14	17	7	42	101	42	243	607	1568	235
1	2	13	17	126	3	103	266	40	619	980	391
5	2	15	19	49	8	103	12008	1	901	28006	29
5	7	6	19	980	1	145	157	134	1375	25552	74
5	42	3	25	2	313	145	22922	1	1399	12008	163
7	4	14	25	1202	1	223	25552	2	1741	3052118	1
7	172	2	31	49	20	259	70340	1	1897	22922	157
13	1	170	31	266	4	265	817	86	2029	2198	1873
13	14	13	31	1568	1	295	172	506	3259	70340	151
13	157	2	37	817	2	373	28006	5	21037	3052118	145
13	2198	1	89	126	63	577	1202	277			

Table 14. (a,b,c) = (2,1,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	4	2	17	1	4	3	11	10	69	3
1	3	2	3	5	4	4	43	1			
2	1	9	3	11	2	10	29	7			

Table 15. (a,b,c) = (2,2,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	5	3	55	1	33	115	19	83	1535	9
1	3	3	7	3	33	41	307	11			
3	1	19	19	807	1	51	127	41			

Table 16.(a,b,c) = (2,3,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	6	4	129	1	14	449	1	148	345	127
1	3	4	8	5	26	17	317	2	364	13953	19
2	1	10	8	205	1	25	33	38			
2	17	2	10	3	67	53	565	10			
4	1	33	10	23	9	58	7095	1			

Table 17. (a,b,c) = (3,1,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	5	2	5	3	5	4	19	13	64	8
1	2	3	2	25	1	5	94	1	13	103	5
1	4	2	3	2	14	6	11	10	17	67	13
2	1	13	3	41	1	6	59	2	17	220	4

Table 18. (a,b,c) = (3,2,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	6	3	82	1	7	206	1	27	2362	1
1	2	4	5	2	38	9	4	61	99	346	85
1	4	3	5	47	2	13	32	16	171	6754	13
3	1	28	7	10	15	17	110	8			

Table 19. (a,b,c) = (3,3,1)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	7	4	1	49	44	6233	1	301	1003	271
1	2	5	4	193	1	46	3281	2	422	18427	29
1	4	4	5	8	10	85	22468	1	787	66370	28
2	1	14	5	188	1	127	550	88			
2	5	4	7	2	74	182	667	149			
2	25	2	13	4	127	241	5623	31			

Table 20. (a,b,c) = (1,1,2)

x	y	z	x	y	z	x	y	z	x	y	z
1	1	4	2	10	1	4	22	1	11	31	4
1	3	2	3	1	10	7	5	10			
2	2	3	4	6	3	9	43	2			

REFERENCES

1. E.S.Barnes, On the Diophantine equation $x^2+y^2+c = xyz$, J. London Math. Soc., 28(1953), 242-244. MR 14, 725.

2. K.Goldberg, M.Newman, E.G.Straus and J.D.Swift, The representation of integers by binary quadratic rational forms, Arch. Math.,5(1954),12-18. MR 15,857.

3. O.Hemer, On the Diophantine equation $y^2-k = x^3$, Ph.D. Diss., Uppasala (1952). MR 14,354.

4. M. Lal, M.F. Jones and W.J.Blundon, Tables of solutions of the Diophantine equation $y^3-x^2 = k$, Department of Mathematics, Memorial University of New foundland, St. John's, New foundland, Canada (1965). MR 33 #91.

5. W.H.Mills, A system of quadratic Diophantine equations, Pacific J.Math., 3(1953), 200-220. MR 14,950.

6. S.P.Mohanty, On the Diophantine equation $y^2-k = x^3$, Ph.D. Diss., UCLA (1971).

7. ____________, A system of cubic Diophantine equations, J. Number Theory, 9(1977), 153-159. MR 56 #248.

8. ____________, On the Diophantine equation $x^3+y+1-xyz = 0$, Math. Student, 45 (1979), 13-16.

9. L.J. Mordell, Diophantine equations, Pure and Appl. Math., Vol. 30, Academic Press, London and New York, 1969. MR 40 #2600.

10. A.Schinzel and W.Sierpinski, Sur l' équation $x^2+y^2+1 = xyz$, Mathematische, Catania 10(1955),30-36. MR 17,711.

11. T.N.Sinha, Note on the Diophantine equation $x^2+y^2+1 = xyz$, Math. Student, 42(1974),73-75. MR 53 # 273.

12. W.R.Utz, Positive solutions of the Diophantine equation $x^3+2y+1-xyz = 0$, Int. J. Math. and Math. Sci.,5(1982), 311-314.

CHAPTER 2

THE DIOPHANTINE EQUATION $(x^2+by)(bx+y^2) = N(x-y)^3$

1. INTRODUCTION

R.J.Stroeker [1] gave a method to obtain all the solutions in non-zero integers of the Diophantine equation

$$(x^2+y)(x+y^2) = N(x-y)^3 \qquad (1)$$

where N is any given non-zero integer. He also gave a table with complete sets of solutions for every N in the range $1 \leq N \leq 51$.

Let N be any given non-zero integer and b any given positive integer. In this chapter we generalize Stroeker's method and show how to secure all the solutions of the Diophantine equation

$$(x^2+by)(bx+y^2) = N(x-y)^3 \qquad (2)$$

in non-zero integers. We prove that all the solutions of (2) can be obtained by the use of the idea of divisibility in integers. We give tables of solutions of (2) for (i) $1 \leq N \leq 100$ and $1 \leq b \leq 4$ and (ii) $1 \leq N \leq 10$ and $5 \leq b \leq 10$. In an appendix we provide a computer program using which all but a few of the solutions of (2) can be obtained for given N and b.

If $x = x_1$, $y = y_1$ is an integral solution of (2), then $x = y_1$, $y = x_1$ is an integral solution of

where $N' = -N$. Hence we assume in the sequel, without loss of generality, that N is positive in (2). If $y = 0$, (2) implies $x = 0$ or $N = b$. If $x = 0$, (2) implies $y = 0$. A solution (x,y) of (2) with $xy \neq 0$ will be referred to as a proper solution. We see that $(x,y) = (-b,-b)$ is always a solution of (2). We shall call this solution the trivial solution of (2). Henceforth we shall consider proper non-trivial solutions of (2).

2. SOLUTIONS IN SOME PARTICULAR CASES

2(α). Below we give a method of solution of (2) for $b = N = 1$, which is different from that of Stroeker's.

THEOREM 2.1. The only proper non-trivial integral solutions of the Diophantine equation

$$(x^2+y)(x+y^2) = (x-y)^3 \tag{3}$$

are $(8,-10)$, $(9,-21)$ and $(9,-6)$.

Proof. We can re-write (3) as

$$y(2y^2+x^2y-3xy+3x^2+x) = 0.$$

Since $y \neq 0$, we have

$$2y^2+(x^2-3x)y+(3x^2+x) = 0. \tag{4}$$

Treating (4) as a quadratic equation in y, we obtain

$$y = \frac{3x-x^2 \pm (x+1)\sqrt{x(x-8)}}{4}. \tag{5}$$

For $x = 8$, we have $y = -10$ and $(x,y) = (8,-10)$ is a solution

of (3). Now consider $x \neq 8$. We must have

$$x(x-8) = \alpha^2 \qquad (6)$$

for some non-zero integer α.

Suppose $\gcd(x, x-8) \neq 1$. Let p be a common prime divisor of x and $x-8$. Then $p|8$ and hence $p = 2$. Letting $x = 2x_1$, $x_1 \neq 4$, we obtain

$$x_1(x_1-4) = \beta^2, \qquad (7)$$

where $\beta = \frac{\alpha}{2}$. If $\gcd(x_1, x_1-4) = 1$, then $x_1 = e^2$, $x_1-4 = f^2$ for some integers e, f. Hence $e^2-f^2 = 4$. This gives $e = \pm 2$, whence $x_1 = 4$, a contradiction. Thus $\gcd(x_1, x_1-4) \neq 1$. Let q be a common prime divisor of x_1 and x_1-4. Then $q|4$ and so $q = 2$. Let $x_1 = 2x_2$, $x_2 \neq 2$. Then we have

$$x_2(x_2-2) = \gamma^2, \qquad (8)$$

where $\gamma = \frac{\beta}{2}$. If $\gcd(x_2, x_2-2) = 1$, then $x_2 = g^2$, $x_2-2 = h^2$ for some integers g, h. So $g^2-h^2 = 2$, which is impossible. Hence $\gcd(x_2, x_2-2) = 2$. Let $x_2 = 2x_3$, $x_3 \neq 1$. Then

$$x_3(x_3-1) = \delta^2 \qquad (9)$$

where $\delta = \frac{\gamma}{2}$. Since $\gcd(x_3, x_3-1) = 1$, we have $x_3 = r^2$ and $x_3-1 = s^2$ for some integers r, s. Consequently $r^2-s^2=1$ and hence $r = \pm 1$. This forces $x_3 = 1$, a contradiction. Hence $\gcd(x, x-8) = 1$. Now (6) implies $x = \lambda^2$ and $x-8 = \rho^2$ for some integers λ, ρ. So $\lambda^2 - \rho^2 = 8$ and hence $\lambda = \pm 3$. This yields $x = 9$ and from (5), $y = -6$ or -21. So $(x,y) = (9,-6)$, $(9,-21)$. Hence the theorem is proved.

In what follows we obtain some results for the existence of proper non-trivial solutions of (2) in certain particular cases.

2(β). Let (x,y) be a proper non-trivial solution of (2) with $y = -b$. Then, since $x \neq -b$, we obtain

$$N = \frac{b(x-b)}{x+b} . \tag{10}$$

Since N and b are positive, $\frac{x-b}{x+b} > 0$. Hence either $x < -b$ or $x > b$. Rewriting (10) as

$$N = b - \frac{2b^2}{x+b} ,$$

We see that $x+b \mid 2b^2$ and thus either $-(2b^2+b) \leq x < -b$ or $b < x \leq 2b^2-b$. Let d be a positive divisor of b. Fix d. The following table gives some particular values of N and x with $y = -b$.

Table 1

Serial No.	N	x
1	$b+d$	$-\frac{b}{d}(2b+d)$
2	$b-d \quad (d < b)$	$\frac{b}{d}(2b-d)$
3	$b+2d$	$-\frac{b}{d}(b+d)$
4	$b-2d \quad (d < \frac{b}{2})$	$\frac{b}{d}(b-d)$
5	$b(d+1)$	$-\frac{b}{d}(d+2)$
6	$b(2d+1)$	$-\frac{b}{d}(d+1)$
7	$\frac{b}{d}(d+1)$	$-b(2d+1)$

Serial No.	N	x
8	$\frac{b}{d}(d+2)$	$-b(d+1)$
9	$\frac{b}{d}(b+d)$	$-(b+2d)$
10	$\frac{b}{d}(2b+d)$	$-(b+d)$
11	$\frac{b}{d}(d-1)$ $(d > 1)$	$b(2d-1)$
12	$\frac{b}{d}(d-2)$ $(d > 2)$	$b(d-1)$

We also see that $N = \frac{b}{d}(2b-d)$ with $d < b$, $y = -(b-d)$ give a proper non-trivial solution of (2) with $x = -b$.

2(γ). Suppose (x,y) is a proper non-trivial solution of (2) with $y = -x$. Then we have

$$N = \frac{(x+b)(x-b)}{8x}. \tag{11}$$

Thus $x \mid b^2$ and $x^2 \equiv b^2 \pmod 8$. So $|x| \leq b^2$ and x,b are of the same parity. When x,b are even, we have $x \equiv b \pmod 4$. If $x = \pm b$, then $N = 0$, a contradiction. So $-b^2 < x < b^2$, with $x \neq \pm b$. For $N = \frac{b^2-1}{8}$ where b odd, $b > 1$, two solutions of (2) with $y = -x$ are given by $x = -1, b^2$. For $b = 3N$, two solutions of (2) with $y = -x$ are given by $x = -N, 9N$.

2(δ). Some polynomial solutions of (2) with $b = N$.

When $b = N$, consider

P_1 : $x = (2N+1)^2$, $\quad y = -N(2N+1)(4N+3)$

P_2 : $x = -(2N-1)^2$, $\quad y = -N(2N-1)(4N-3)$ $\quad (N > 1)$

P_3 : $x = 2(N+1)^2$, $\quad y = -N(N+1)(2N+3)$

P_4 : $x = -2(N-1)^2$, $\quad y = -(N-1)N(2N-3)$ $\quad (N > 2)$

P_5 : $x = (N+2)^2$, $\quad y = \dfrac{-N(N+2)(N+3)}{2}$

P_6 : $x = -(N-2)^2$, $\quad y = \dfrac{-N(N-3)(N-2)}{2}$ $\quad (N > 3)$

P_7 : $x = 8N$, $\quad y = -10N$

P_8 : $x = 9N$, $\quad y = -21N$

P_9 : $x = 9N$, $\quad y = -6N$.

One can see that each $P_i (i = 1, \ldots, 9)$ is a solution of (2) with $b = N$. For example, consider P_6. We get

$$x^2 + by = \frac{(N-4)^2(N-2)(N-1)}{2}$$

and

$$y^2 + bx = \frac{(N-4)(N-2)^2(N-1)^2 N}{4}.$$

So

$$(x^2+by)(y^2+bx) = \frac{(N-4)^3(N-2)^3(N-1)^3 N}{8} = N(x-y)^3,$$

establishing our claim. However, $\{P_i\}$ given by us is not an exhaustive list of solutions of (2) with $b = N$.

Now we have some lemmas.

LEMMA 2.2. If $N \equiv \pm b \pmod 4$, $N \neq b$, then (2) has at least one proper non-trivial solution. If, in addition, b is even, then (2) has at least two proper non-trivial solutions.

Proof. When $N \equiv b \pmod 4$, we have a solution $(x,y) = (\frac{N+b}{2}, \frac{N-b}{4})$. When $N \equiv -b \pmod 4$, consider $(x,y) = (-(\frac{N+b}{4}), \frac{b-N}{2})$.

REMARK. In particular, when $b = 1$, $N > 1$ and N odd, (2) has at least one proper non-trivial solution, a result which was obtained by R.J.Stroeker.

Some proper non-trivial solutions of (2) are given by the following

LEMMA 2.3.

(i) If $b = 3N$ and N odd, $(x,y) = (-N,N)$, $(6N,-3N)$, $(9N,-9N)$; if $b = 3N$ and N even, $(x,y) = (-18N, \frac{9N}{2})$, $(-3N, \frac{3N}{2})$, $(-N,N)$, $(2N, -\frac{N}{2})$, $(6N,-3N)$, $(9N,-9N)$

(ii) If $b > 1$ and $N = b(2b-1)$, $(x,y) = (-b, 1-b)$

(iii) If $b > 2$ and $N = b(b-1)$, $(x,y) = (-b, 2-b)$

(iv) If b even and $N = 5b$, $(x,y) = (-\frac{3b}{2}, -b)$

(v) If b even and $N = \frac{15b}{2}$, $(x,y) = (-4b, -8b)$

(vi) If $b = 4t+1$ where t is an integer > 0 and $N = 18t^2+9t+1$, $(x,y) = (-(4t+2), -4t)$

(vii) If $b = 4t+3$, $t \geq 0$ and $N = 18t^2+27t+10$, $(x,y) = (-(4t+4), -(4t+2))$

(viii) If $b = 6t+3$, $t \geq 0$ and $N = 30t+15$, $(x,y) = (-(6t+3), -(4t+2))$

(ix) If $b \equiv 2,3,5,6 \pmod 8$, $b > 2$ and

$N = \frac{1}{16}(b^4+3b^2+4)$, $(x,y) = (b+2,b-2)$

(x) If $N = t^4+(2b+2)t^3+(b^2+3b+1)t^2+(b^2+3b)t+b$, $t > 0$, $(x,y) = (t+1,t)$

(xi) If $N = 2t^4+(2b+4)t^3+(b^2+6b)\frac{t(t+1)}{2} + 2t^2+b$, $t > 0$, $(x,y) = (2t+2,2t)$.

LEMMA 2.4. Suppose $b \neq N, 3N$ and $N > 1$. If $27N^2-2b^2$ is a square, then there are at least four proper non-trivial solutions of (2).

Proof. Suppose

$$27N^2-2b^2 = r^2 \tag{12}$$

for some integer r. If r is odd, then N is odd. So $N^2 \equiv 1 \pmod 4$. This gives $2b^2 \equiv 2 \pmod 4$ and hence b is odd. If r is even, then N is even. So $2b^2 \equiv 0 \pmod 4$ and hence b is even. Thus $r \equiv N \equiv b \pmod 2$. Since $b \neq 3N$, we have $r \neq \pm 3N$. Consider

P_1 : $x = \frac{9N-b+2r}{2}$, $y = \frac{-9N+2b-r}{2}$

P_2 : $x = \frac{9N-b-2r}{2}$, $y = \frac{-9N+2b+r}{2}$

P_3 : $x = \frac{9N+2b+r}{2}$, $y = -\frac{(9N+b+2r)}{2}$

P_4 : $x = \frac{9N+2b-r}{2}$, $y = \frac{-9N-b+2r}{2}$

Since $r \equiv N \equiv b \pmod 2$, the coordinates in each P_i $(i = 1,\ldots,4)$ are integers.

One can check that each $P_i (i = 1,\ldots,4)$ a solution of (2). For example, let us consider P_1. In this case

$$x^2+by = \frac{81N^2+5b^2+4r^2-36bN-6br+36rN}{4}$$

and

$$y^2+bx = \frac{81N^2+2b^2+r^2-18bN+18Nr}{4}.$$

Using (12) we get

$$x^2+by = \frac{3(6N-b+r)^2}{4}$$

and

$$y^2+bx = \frac{9N(6N-b+r)}{2}.$$

Hence

$$(x^2+by)(y^2+bx) = \frac{27N(6N-b+r)^3}{8} = N(x-y)^3,$$

thus proving our claim.

Next we assert that each P_i is proper. If x in P_1 or P_2 is 0, then $r^2 = (\frac{b-9N}{2})^2$ and so $(3N-b)(N+b) = 0$. Since N+b is positive, we have $b = 3N$, a contradiction. If x in P_3 or P_4 is 0, then $r^2 = (9N+2b)^2$. This yields $32N^2+18bN+3b^2 = 0$, a contradiction. If y in P_1 or P_2 is 0, then $r^2 = (2b-9N)^2$ and so $32N^2-18bN+3b^2 = 0$. This yields $N = \frac{9 \pm \sqrt{-15}}{32}b$, a contradiction. If y in P_3 or P_4 is 0, then $(3N+b)(N-b) = 0$. Since $3N+b \neq 0$, we obtain $b = N$, a contradiction.

Next we assert that each P_i is non-trivial. If P_1 or P_2 is trivial, we get $b = N$, a contradiction. If P_3 or P_4 is trivial, we obtain $9N+7b = 0$, a contradiction again.

Next we assert that all the four P_i's are distinct. If $P_1 = P_2$ or $P_3 = P_4$, then $r = 0$. Hence $27N^2-2b^2 = 0$. This implies N is even. Let $N = 2N_1$, where N_1 is an integer. Then $b = \sqrt{54}\ N_1$, a contradiction. If $P_1 = P_3$ or $P_2 = P_4$, then $r = 3b$ and so $27N^2-11b^2 = 0$. This forces $11 \mid N$. Let $N = 11N_1$. Then $b = \sqrt{297}\ N_1$, a contradiction. If $P_1 = P_4$ or $P_2 = P_3$, then $r^2 = b^2$. This yields $b = 3N$, a contradiction. This completes the proof of Lemma 2.4.

From Lemmas 2.2 and 2.4, we deduce the following corollary, which was obtained by R.J.Stroeker.

COROLLARY 2.5. If $N > 1$ and $27N^2-2$ is a square, then there are at least five proper non-trivial solutions of (1).

COROLLARY 2.6. Given b, there are infinitely many values of N for which (2) has at least five non-zero integral solutions.

PROOF. Given b, one can check that $N = 51b$, $r = 265b$ always satisfy (12). If $3 \mid b$, let $b = 3b_1$. Then $N = 11b_1$, $r = 57b_1$ also satisfy (12). Whenever N and r satisfy (12), we see that $N_1 = 26N+5r$, $r_1 = 135N+26r$ also satisfy (12).

LEMMA 2.7. If (x,y) is a solution of (2) and t is any given positive integer, then $X = tx$, $Y = ty$ is a solution of

$$(X^2+b_1Y)(b_1X+Y^2) = N_1(X-Y)^3$$

where $b_1 = bt$, $N_1 = Nt$.

3. METHOD OF SOLVING THE TITLE EQUATION

LEMMA 2.8. Let (x,y) be a proper non-trivial integral solution of (2) with $N > 0$. Then there are non-zero integers u,v and w satisfying

$$2x = v-u+w+b,\ 2y = v-u-w+b \tag{13}$$

$$uv = Nw \tag{14}$$

and

$$(u+v-w)^2 = 4(u-b)(v+b)+b^2. \tag{15}$$

Conversely, for any triad (u,v,w) of non-zero integers satisfying (14) and (15), the relations (13) define a proper non-trivial solution (x,y) of (2) with $N > 0$.

Proof. Let (x,y) be a proper non-trivial integral solution of (2) with $N > 0$. Substituting $k = x^2+by$, $w = x-y$ and $m = x+y-b$, we have

$$bx+y^2 = k-mw. \tag{16}$$

If $w = 0$, then $w = x-y$ implies $x = y$ and so (2) implies $(x,y) = (0,0)$ or $(-b,-b)$, a contradiction. So $w \neq 0$. From the above relations, we obtain

$$2x = w+m+b,\ 2y = -w+m+b \tag{17}$$

and

$$4k = (w+m)^2+4bm+3b^2. \tag{18}$$

Hence (2) becomes

$$k^2-kmw-Nw^3 = 0. \qquad (19)$$

Considering (19) as a quadratic equation in k, we conclude that

$$m^2+4Nw = A^2 \qquad (20)$$

for some rational integer A. Choose the sign of A such that

$$2k = (A+m)w.$$

From (20) we have

$$(A+m)(A-m) = 4Nw$$

and hence there are rational integers u and v such that

$$A-m = 2u, \ A+m = 2v, \ uv = Nw.$$

If $u = 0$ or $v = 0$, then $A^2 = m^2$ and so (20) implies $w = 0$, a contradiction. So $uv \neq 0$. Now $k = vw$ and $m = v-u$. Hence (18) yields (15).

For the converse, given $u \neq 0$, $v \neq 0$, suppose there exist $w_1, w_2 \neq 0$ satisfying (14) and (15). Then $uv = Nw_1$ and $uv = Nw_2$. This implies $w_1 = w_2$. Hence for each pair $(u,v) \neq (0,0)$, there is at most one $w \neq 0$ such that (14) and (15) are satisfied. Consequently each pair (u,v)w $uv \neq 0$ and satisfying (14) and (15), determines uniquely a proper non-trivial solution of (2).

Now we discuss the method of obtaining all the proper non-trivial solutions of (2). Hereafter u,v,w

From (15) it follows that

$$4(u-b)(v+b) \geq -b^2.$$

i.e.,

$$(u-b)(v+b) \geq -\left[\frac{b^2}{4}\right]$$

where $[x]$ denotes the greatest integer not greater than x. There are three possibilities :-

I. $(u-b)(v+b) = -1, -2, \ldots, -\left[\frac{b^2}{4}\right]$ such that $4(u-b)(v+b)+b^2$ is a square.

II. $(u-b)(v+b) = 0$

III. $(u-b)(v+b) > 0$.

We discuss them one by one.

I. $(u-b)(v+b) = -1, -2, \ldots, -\left[\frac{b^2}{4}\right]$ such that $4(u-b)(v+b)+b^2$ is a square. This does not occur for $b = 1$. For $b > 1$, this implies

$$(u-b)(v+b) = -j(b-j)$$

where $1 \leq j \leq \left[\frac{b}{2}\right]$. Fix j. We note that $u-b \mid j(b-j)$ and $v+b \mid j(b-j)$ and hence we can find u and v. Also

$$(u+v-w)^2 = (b-2j)^2.$$

Hence $u+v-w = b-2j$ or $2j-b$. This implies $w = u+v-b+2j$ or $w = u+v+b-2j$ and so W can be evaluated. We find N using (14) and x, y using (13). Hence

$$N = \frac{uv}{u+v-b+2j}, \quad x = v+j, y = b-u-j$$

or

$$N = \frac{uv}{u+v+b-2j}, \quad x = v-j+b, \quad y = j-u$$

where $u+v-b+2j$, $u+v+b-2j$, $v+j$, $j-u$, $b-u-j$, $v-j+b$ are all non-zero.

When b is even, if $u+v = 0$ and $j = \frac{b}{2}$, then $w = 0$, a contradiction. In particular, when b is even, we cannot have $(u,v) = (\frac{3b}{2}, \frac{-3b}{2}), (\frac{b}{2}, \frac{-b}{2})$.

II. $(u-b)(v+b) = 0$. This implies $u = b$ and v arbitrary or $v = -b$ and u arbitrary.

II (i). $u = b$. In this case

$$(b+v-w)^2 = b^2.$$

Hence $v = w$ or $w-2b$. If $v = w$, then $y = 0$, a contradiction. Thus $v = w-2b$. Now

$$N = \frac{b(w-2b)}{w} = b - \frac{2b^2}{w}.$$

Thus $w \mid 2b^2$ and either $w < 0$ or $b > \frac{2b^2}{w}$, i.e., $w > 2b$. We obtain

$$x = w-b, \quad y = -b.$$

II(ii). $v = -b$. In this case

$$(u-b-w)^2 = b^2.$$

Hence $u = w$ or $w+2b$. If $u = w$, then $x = 0$, a contradiction. So $u = w+2b$. Consequently

$$N = \frac{-b(w+2b)}{w} = -\frac{2b^2}{w} - b.$$

Thus $w \mid 2b^2$ and $-2b < w < 0$. If $w = -b$, then $u = b$ and so $y = 0$, a contradiction. Hence $w \neq -b$. We obtain

$$x = -b, \quad y = -(w+b).$$

III. The possibility III i.e., $(u-b)(v+b) > 0$ can be restated as follows :-

III(a) $u < 0$, $v < -b$

III(b) $u = 1,2,3,\ldots, b-1$ with $b > 1$ and v arbitrary but $v < -b$

III(c) $v = -1,-2,-3,\ldots,-(b-1)$ with $b > 1$ and u arbitrary but $u > b$.

III(d) $u > b$, $v > 0$.

We discuss them one by one.

III(a). $u < 0$, $v < -b$. In this case $uv > b$. Hence (14) implies $w > 0$. We can rewrite (15) as

$$w(w-2(u+v)) = b^2-(u-v-2b)^2. \qquad (21)$$

Since $u < 0$, $v < -b$, we have $u+v < -b < 0$ and $w-2(u+v) > w+2b > 0$. Hence (21) implies $b^2 > (u-v-2b)^2$. So $u-v = 2b+s$ where $s = 0, \pm 1, \pm 2, \ldots, \pm (b-1)$. Fix s. We have

$$w(w-2(u+v)) = b^2-s^2.$$

Thus $w \mid b^2-s^2$. Let d be a positive divisor of b^2-s^2. Fix d and take $w = d$. Then $d-2(u+v) = \dfrac{b^2-s^2}{d}$ and hence $u+v = \dfrac{d^2+s^2-b^2}{2d}$. This implies either all of b,s,d are even

or one of them even and the other two odd. Now $u+v < -(b+1)$, $d > 0$ imply $d^2+s^2-b^2 < -2d(b+1)$ i.e., The restriction for d is given by the inequality

$d(2b+d+2) < b^2-s^2$. We have

$$u = \frac{d^2+s^2-b^2+2sd+4bd}{4d}$$

and

$$v = \frac{d^2+s^2-b^2-2sd-4bd}{4d}.$$

Using (14), we get $N = \frac{uv}{d}$. We obtain

$$x = \frac{d-(b+s)}{2}, \quad y = \frac{-(d+b+s)}{2},$$

using (13).

III(b). $u = 1,2,..,(b-1)$ with $b > 1$ and v is arbitrary but $v < -b$. In this case $uv < -b$. Hence (14) implies $w < 0$. Fix u and put

$$v_1^2 = 4(u-b)(v+b)+b^2. \tag{22}$$

Then

$$v = \frac{v_1^2-4bu+3b^2}{4(u-b)}. \tag{23}$$

Since $v < -b$, we obtain

$$|v_1| > b. \tag{24}$$

Now (15) implies

either $\quad w = u+v+v_1$

or $\quad w = u+v-v_1$.

Hence we have either

$$w = u+v_1+ \frac{v_1^2-4bu+3b^2}{4(u-b)} \qquad (25)$$

or

$$w = u-v_1+ \frac{v_1^2-4bu+3b^2}{4(u-b)} . \qquad (25')$$

First we consider (25). Using this and (23) in (14) we obtain

$$(N-u)v_1^2+4N(u-b)v_1+\{ 4Nu(u-b)+b(N-u)(3b-4u) \} = 0 \qquad (26)$$

If $N = u$, then (26) implies $v_1 = -u$. Hence $|v_1| < b$, which contradicts (24). This forces $N \neq u$. So (26) is a quadratic equation in v_1 and thus we have

$$v_1 = \frac{2N(b-u) \pm \sqrt{4N^2(b-u)^2-(N-u)\{ 4Nu(u-b)+b(N-u)(3b-4u)\}}}{N-u}$$

This implies that the expression within the radical sign must be a perfect square. i.e.,

$$b^2N^2+2u(2u^2-6bu+3b^2)N-bu^2(3b-4u) = E^2 \qquad (27)$$

for some integer E. Multiplying both sides of (27) by b^2 and rearranging, we obtain

$$(b^2N+2u^3-6bu^2+3b^2u)^2-(bE)^2 = 4u^2(b-u)^3(3b-u).$$

i.e.,

$$(b^2N+2u^3-6bu^2+3b^2u+bE)(b^2N+2u^3-6bu^2+3b^2u-bE)=4u^2(b-u)^3(3b-u). \qquad (28)$$

Thus the two factors in the L.H.S. of (28) are divisors of $4u^2(b-u)^3(3b-u)$ and so N and E can be found. Now we have

$$v_1 = \frac{2N(b-u) \pm E}{N-u}.$$

Hence we restrict to those values of N and E which satisfy

$$N-u \mid 2N(b-u) \pm E. \qquad (29)$$

Thus we find v_1 and using this in (23) and (25) we obtain v and w. By means of (13) we find x and y.

Next we consider (25′). Because of (23) and (25′), the equation (14) is transformed as

$$(N-u)v_1^2+4N(b-u)v_1+\{4Nu(u-b)+b(N-u)(3b-4u)\} = 0. \qquad (26')$$

Using (24), one can check that $N \neq u$. As (26) and (26′) differ only in the sign of v_1, we have

$$v_1 = \frac{2N(u-b) \pm E}{N-u}$$

where N and E are got from (28) with the restriction given by

$$N-u \mid 2N(u-b) \pm E. \qquad (29')$$

(25) and (25′) together give $v_1 = \dfrac{\pm 2N(b-u) \pm E}{N-u}$. Because of (23), it is enough to consider $v_1 = \dfrac{2N(b-u) \pm E}{N-u}$. We can find w, x and y.

III(c). $v = -1, -2, \ldots, -(b-1)$ with $b > 1$ and u is arbitrary but $u > b$. In this case $uv < -b$ and so from (14) we have

$w < 0$. Fix v and put

$$u_1^2 = 4(u-b)(v+b)+b^2 \tag{30}$$

Then

$$u = \frac{u_1^2+4bv+3b^2}{4(v+b)}. \tag{31}$$

Because $u > b$, we get

$$|u_1| > b. \tag{32}$$

Now (15) implies either

$$w = v+u_1+\frac{u_1^2+4bv+3b^2}{4(v+b)} \tag{33}$$

or

$$w = v-u_1+\frac{u_1^2+4bv+3b^2}{4(v+b)}. \tag{33'}$$

First we consider (33). In view of this and (31), the equation (14) becomes

$$(N-v)u_1^2+4N(b+v)u_1+\{4Nv(b+v)+b(N-v)(3b+4v)\} = 0. \tag{34}$$

If $N = v$, then (34) implies $u_1 = -v$ and so $|u_1| < b$, which contradicts (32). Consequently $N \neq v$. Considering (34) as a quadratic equation in u_1 we have

$$b^2N^2+2v(2v^2+6bv+3b^2)N-bv^2(3b+4v) = F^2 \tag{35}$$

for some integer F. From (35) we get

$$(b^2N+2v^3+6bv^2+3b^2v)^2-(bF)^2 = 4v^2(b+v)^3(3b+v).$$

i.e.,

$$(b^2N+2v^3+6bv^2+3b^2v+bF)(b^2N+2v^3+6bv^2+3b^2v-bF) = 4v^2(b+v)^3(3b+v). \tag{36}$$

Thus the two factors in the L.H.S. of (36) are divisors of $4v^2(b+v)^3(3b+v)$ and hence we can find N and F. Now we have

$$u_1 = \frac{-2N(v+b)\pm F}{N-v}.$$

Hence we restrict to those values of N and F which satisfy

$$N-v \mid 2N(v+b)\pm F. \tag{37}$$

Thus we find u_1 and using this in (31) and (33) we get u and w. We find x and y from (13).

Next we consider (33′). Using this and (31) a in (14), we get

$$(N-v)u_1^2-4N(b+v)u_1+\{4Nv(b+v)+b(N-v)(3b+4v)\}=0. \tag{34′}$$

Because of (32), we have $N \neq v$. As before we obtain

$$u_1 = \frac{2N(v+b)\pm F}{N-v}$$

where N and F are got from (36) with the restriction given by

$$N-v \mid 2N(v+b) \pm F. \tag{37′}$$

(33) and (33′) together give $u_1 = \dfrac{\pm 2N(v+b)\pm F}{N-v}$. Because of (31), it is enough to consider $u_1 = \dfrac{2N(v+b)\pm F}{N-v}$. We can find w, x and y.

III(d). $u > b$, $v > o$. In this case $uv > b$. Hence (14) implies $w > o$. Now there are three possibilities:

(i) $w = 2(u+v)$, (ii) $w > 2(u+v)$, (iii) $w < 2(u+v)$.

We discuss them one by one.

III d(i). $w = 2(u+v)$. In this case (21) implies

$$b^2 = (u-v-2b)^2.$$

So $u-v = b$ or $3b$. First suppose $u-v = b$. Then $4u = w+2b$ and $4v = w-2b$. Hence (15) implies

$$w^2-16Nw-4b^2 = 0.$$

Hence $w = 8N \pm 2\sqrt{16N^2+b^2}$. This implies

$$16N^2+b^2 = G^2$$

for some integer G. i.e.,

$$(G+4N)(G-4N) = b^2.$$

Hence $G+4N$ and $G-4N$ are divisors of b^2. Now $u > b$, $v > 0$ imply $u+v > b+1$ and so $w > 2b+2$. Hence we restrict to those N and G which satisfy $4N \pm G > b+1$. We get $x = \frac{w}{2}$ and $y = -\frac{w}{2}$.

Next suppose $u-v = 3b$. Then $4u = w+6b$ and $4v = w-6b$. Hence (14) implies

$$w^2-16Nw-36b^2 = 0.$$

This gives $w = 8N \pm 2\sqrt{16N^2+9b^2}$ and hence

$$16N^2+9b^2 = H^2$$

for some integer H. i.e.,

$$(H+4N)(H-4N) = 9b^2 .$$

Thus H+4N and H-4N are divisors of $9b^2$. We restrict to N and H satisfying $4N \pm H > b+1$. We obtain $x = \frac{w}{2} - b$ and $y = -\frac{w}{2} - b$.

III d(ii). $w > 2(u+v)$. In this case (21) implies

$$b^2 > (u-v-2b)^2 .$$

Hence the discussion for III(a) carries over to the present situation, with a variation in the inequality for d in terms of b and s. In III(a) we had

$$d(2b+d+2) < b^2 - s^2 .$$

In the present case we have $u+v > b+1$ and so

$$d(d-2b-2) > b^2 - s^2 .$$

III (d) (iii). $w < 2(u+v)$. For this case we have the following important

LEMMA 2.9. $\min(u,v) < 4N$.

Proof. Using $w < 2(u+v)$ and (14) we have

$$\frac{uv}{u+v} < 2N.$$

This implies

$$\min(u,v) < 4N.$$

Now we consider the proper non-trivial solutions of (2) in two special cases, viz. (i) $u = N$, (2) $v = N$.

First suppose $u = N$. Then $w = v$. Hence (15) becomes

$$N^2-b^2 = 4(N-b)(v+b).$$

Since $u > b$ we have $N > b$. This implies

$$v = \frac{N-3b}{4} < u.$$

Hence in this case max $(u,v) = N$ and $x = \frac{-(b+N)}{4}$, $y = \frac{b-N}{2}$.

Next suppose $v = N$. Then $w = u$. Hence (15) implies

$$N^2-b^2 = 4(u-b)(N+b).$$

Consequently we have $u = \frac{N+3b}{4}$. Now $u > b$ implies $N > b$. This forces $u < N$. Hence in this case max $(u,v) = N$ and $x = \frac{b+N}{2}$, $y = \frac{N-b}{4}$. Thus we have proved the following

LEMMA 2.10. (for III (d) (iii)) If $u = N$ or $v = N$, then max $(u,v) = N$.

Next we consider the proper non-trivial solutions of (2) when $u = 3b \neq N$. For this case put

$$v_1^2 = 4(u-b)(v+b)+b^2. \tag{22a}$$

Then

$$v = \frac{v_1^2-9b^2}{8b} \tag{23a}$$

and (15) implies

either $\quad w = u+v+v_1$

or $\quad w = u+v-v_1$.

Hence we have either

$$w = \frac{(v_1+3b)(v_1+5b)}{8b} \tag{25a}$$

or

$$w = \frac{(v_1-3b)(v_1-5b)}{8b} . \tag{25'a}$$

First we consider (25a). Using this and (23a) in (14) we have $v_1 = \frac{b(9b+5N)}{3b-N}$, i.e.,

$$v_1 = \frac{24b^2}{3b-N} - 5b.$$

Thus $3b-N \mid 24b^2$. We get $v = \frac{2bN(N+9b)}{(N-3b)^2}$ and $w = \frac{6b^2(N+9b)}{(N-3b)^2}$.
Hence $x = \frac{18b^2(N+b)}{(N-3b)^2}$ and $y = \frac{12b^2}{N-3b}$. We shall take the integral values for x and y.

Next we consider (25'a). Using this and (23a) in (14) we obtain $v_1 = \frac{b(5N+9b)}{N-3b}$ i.e.,

$$v_1 = 5b + \frac{24b^2}{N-3b} .$$

Thus $N-3b \mid 24b^2$.

We get the same v,w and consequently the same x and y as for (25a).

Now we show how to find the proper non-trivial solutions of (2) in Case III (d) (iii). The solutions in this case can be classified into two classes: - 1. Solutions with $u \le v$; 2. Solutions with $v \le u$. In the former case we have $u < 4N$ by Lemma 2.9. and in the latter case we have $v < 4N$. Assume that $u \neq 3b, N$ and $v \neq N$. We can now obtain

the solutions by proceeding exactly as in III(b) and III(c). As we have assumed $u \neq N, v \neq N$, the inequalities (24) and (32) are not necessary now.

For given b we obtain all the proper non-trivial solutions of (2) by considering the cases I, II, III(a)-(d). In each case the solutions are obtained by considering the divisors of certain functions of b and so the number of solutions in each case is finite. Thus we have established the following.

THEOREM 2.11. For any given positive integers b and N, the equation (2) has only a finite number of proper non-trivial integral solutions.

Next we shall obtain a bound for the size of the solutions of (2) in Case III(d) (iii) by assuming $u \neq N$, $v \neq N$ and discarding the values assumed by N when $u = b+1,\ldots,3b$ so that $u > 3b$. First we shall show that

$$|u-N| \geq 3$$

and

$$|v-N| \geq 3$$

provided that $N \geq 3b+3$ with $b = 1,2,3$ or $N \geq 4b$ with $b \geq 4$.

Eliminating w from (14) and (15) we obtain

$$(uN+vN-uv)^2 = 4N^2(u-b)(v+b)+b^2N^2.$$

This can be rewritten as

$$(N-v)^2u^2-2N(v^2+vN+2bN)u+N^2(v+b)(v+3b) = 0$$

or as

$$(N-u)^2v^2-2N(u^2+uN-2bN)v+N^2(u-b)(u-3b) = 0.$$

First consider (38). This implies that $u \mid N$ and $N \mid (N-v)^2u^2$. Dividing (38) throughout by uN, w

$$\frac{(N-v)^2u}{N} -2(u^2+vN+2bN)+\frac{N(v+b)(v+3b)}{u} = 0.$$

This implies that $\frac{u(N-v)^2}{N}$ is an integer. Put

$$\delta_1 = \frac{u(N-v)^2}{N} .$$

Then

$$(N-v)^2 = \frac{N\delta_1}{u} .$$

Hence (38) becomes

$$\delta_1u-2(v^2+vN+2bN)u+N(v+b)(v+3b) = 0.$$

This implies that

$$\frac{N(v+b)(v+3b)}{u}$$

is an integer. Put

$$\delta_2 = \frac{N(v+b)(v+3b)}{u}$$

so that

$$\delta_1+\delta_2 = 2(v^2+vN+2bN)$$

and

$$\delta_1\delta_2 = (N-v)^2(v+b)(v+3b).$$

Clearly $\delta_1\delta_2 > 0$. We have

$$[\delta_1 - \tfrac{1}{2}(N-v)^2]\,[\,\delta_2 - \tfrac{1}{2}(N-v)^2]$$

$$= (N-v)^2[\,(\tfrac{1}{2}v+b)(v-N+2)+v(3b-1)+b(3b-2)+\tfrac{1}{16}(N-v)^2\,].$$

If $N \geq 4b$, we assert that $|v-N| \geq 3$. Suppose $0 < |v-N| \leq 2$ and $N \geq 4b$. Then we have

$$[\,\delta_1 - \tfrac{1}{2}(v-N)^2][\,\delta_2 - \tfrac{1}{2}(v-N)^2\,] < 0$$

and

$$[\,\delta_1 - \tfrac{1}{4}(v-N)^2]\,[\delta_2 - \tfrac{1}{4}(v-N)^2\,] > 0.$$

This implies

$$\tfrac{1}{4}(v-N)^2 < \delta_i < \tfrac{1}{2}(v-N)^2$$

for either $i = 1$ or $i = 2$, a contradiction. Hence $N \geq 4b$ implies that $|v-N| \geq 3$.

Next consider (39). This implies that $\frac{v(N-u)^2}{N}$ is an integer. Put

$$\varepsilon_1 = \frac{v(N-u)^2}{N}.$$

Then we have

$$\varepsilon_1 v - 2(u^2+uN-2bN)v + N(u-b)(u-3b) = 0.$$

This implies that

$$\frac{N(u-b)(u-3b)}{v}$$

is an integer. Put

$$\varepsilon_2 = \frac{N(u-b)(u-3b)}{v} .$$

Then $\varepsilon_1+\varepsilon_2 = 2(u^2+uN-2bN)$

and $\varepsilon_1\varepsilon_2 = (N-u)^2(u-b)(u-3b).$

Since $u \geq 3b$, we have $\varepsilon_1\varepsilon_2 \geq 0$. Now

$$[\ \varepsilon_1 - \tfrac{1}{4}(N-u)^2]\ [\varepsilon_2 - \tfrac{1}{4}(N-u)^2\ ]$$

$$= (N-u)^2\ [(\ \tfrac{1}{2}u-b)(u-N-2)-(3b-1)(u-b)-b+\tfrac{1}{16}(u-N)^2\ ].$$

If $0 < |u-N| \leq 2$ then

$$[\ \varepsilon_1 - \tfrac{1}{4}(N-u)^2]\ [\ \varepsilon_2 - \tfrac{1}{4}(N-u)^2\ ] < 0$$

and hence

$$0 \leq \varepsilon_i < \tfrac{1}{4}(u-N)^2 = 1$$

for either $i = 1$ or $i = 2$. This implies $\varepsilon_1\varepsilon_2 = 0$. Consequently $u = 3b$, a contradiction to our assumption. For $|u-N| = 2$ and $u = 3b$, we have $N = 3b\pm1, 3b\pm2$. Hence we consider $N \geq 3b+3$ so that $\varepsilon_1\varepsilon_2 > 0$. This implies $|u-N| \geq 3$. Thus, if $N \geq 3b+3$ with $b = 1,2,3$ or if $N \geq 4b$ with $b \geq 4$, then we have

$$|v-N| \geq 3 \text{ and } |u-N| \geq 3.$$

Now consider (38) and put

$$f(x) = \frac{x^2+xN+2bN}{(x-N)^2} .$$

Then

$$\frac{df(x)}{dx} = \frac{3Nx+N^2+4bN}{(n-x)^3} .$$

Hence the function f(x) is increasing on (0,N) and decreasing on (N, ∞). In view of this (38) implies that

$$u < \frac{2N(v^2+vN+2bN)}{(N-v)^2}$$

i.e.,

$$u \leq \frac{2}{3}N\left(\frac{2}{3}N^2+3N+\frac{2}{3}bN+3\right)$$

$$= \frac{2}{3}N\left[N^2-\frac{1}{3}(N+1)(N-2b-10)-\frac{1}{3}(2bN+1)\right].$$

Hence

$$u < \frac{2}{3}N^3 \text{ if } N \geq 2(b+5).$$

Next consider (39) and put

$$g(x) = \frac{x^2+xN-2bN}{(x-N)^2}.$$

Then

$$\frac{dg(x)}{dx} = \frac{3Nx+N^2-4bN}{(N-x)^3}.$$

So the function g(x) is increasing on (0,N) and decreasing on (N, ∞). Hence (39) implies that

$$v < \frac{2N(u^2+uN-2bN)}{(N-u)^2}.$$

i.e.,

$$v \leq \frac{2}{3}N\left(\frac{2}{3}N^2+3N-\frac{2}{3}bN+3\right)$$

$$= \frac{2}{3}N\left[N^2-\frac{1}{3}(N-9)(N+2b)-3(2b-1)\right].$$

Hence

$$v \leq \frac{2}{3}N^3 \text{ if } N \geq 9$$

and so we have max $(u,v) < \frac{2}{3}N^3$ if $N \geq 2(b+5)$. It remains to check that max $(u,v) < \frac{2}{3}N^3$ in the cases $N < 2(b+5)$. The exceptions for this with $b = 1, \ldots, 10$ are given in the following table.

Table 2

b	N	(u,v)
1	1	(1,2),(1,3),(3,5),(6,3),(15,2)
	2	(16,5)
	4	(3,104)
2	1	(2,4)
	2	(2,5),(2,6),(2,7),(6,10),(12,6),(30,4),(42,1),(90,3)
	3	(6,28),(8,18)
	4	(6,88)
	5	(6,460)
	7	(6,700)
	8	(6,208)
3	1	(3,3),(6,3)
	2	(3,12)
	3	(18,9),(30,1),(30,7),(45,6),(84,5),(165,2),(273,4)
	7	(9,357)
	8	(9,1680)
	10	(9,2220)

b	N	(u,v)
4	2	(4,8)
	3	(4,24)
	4	(60,8),(84,2),(180,6),(420,3),(612,5)
	11	(12,4136)
	13	(12,5096)
5	2	(8,7),(20,5)
	3	(33,7)
	5	(105,9),(180,3),(330,7),(855,4),(1155,6)
	11	(110,5)
	13	(15,1885)
	14	(15,8260)
	16	(15,9760)
	17	(15,2635)
6	2	(6,6),(12,6)
	6	(168,10),(330,4),(546,8),(1518,5),(1950,7)
	17	(18,14484)
	19	(18,16644)
7	3	(117,5)
	4	(112,7)
	7	(252,11),(546,5),(840,9),(2457,6),(3045,8)
	20	(21,23240)
	22	(21,26180)
8	8	(360,12),(840,6),(1224,10),(3720,7),(4488,9)
	22	(24,8272)
	23	(24,34960)
	25	(24,38800)

b	N	(u,v)
9	3	(18,9)
	9	(495,6),(495,13),(819,12),(1224,7),(1710,11), (5355,8),(6327,10)
	25	(27,11925)
	26	(27,50076)
10	10	(1710,8),(2310,12),(7410,9),(8610,11)
	28	(30,16520)
	29	(30,69020)

In the above discussion, we have assumed that $u \neq 3b$. If $u = 3b$, then $v = 2bN(N+9b)$ leads to a solution of (2) for $N = 3b \pm 1$. In this case $\max(u,v) > \frac{2}{3}N^3$.

THEOREM 2.12. If (x,y) is a proper non-trivial solution of (2), then

$$\max(|x|, |y|) < N^3$$

if $N \geq 10$ and $N > \frac{b}{4}$.

Proof. With the assumptions $u > b$, $v > 0$, $w < 2(u+v)$, we have proved that $\min(u,v) < 4N$ and by assuming further that $u > 3b$ and $N \geq 2(b+5)$, we have proved that $\max(u,v) < \frac{2}{3}N^3$. Hence

$$w \leq 2(u+v) = 2(\min(u,v)+\max(u,v)$$

$$< 2(4N+\tfrac{2}{3}N^3).$$

We have

$$(2x+b)^2 = 4w(v+b)+b^2$$

and

$$(2y+b)^2 = 4w(u-b)+b^2 .$$

Hence

$$\max((2x+b)^2,(2y+b))^2 = \max(4w(v+b)+b^2,4w(u-b)+b^2)$$

$$< 8(\tfrac{2}{3}N^3+4N)(\tfrac{2}{3}N^3+b)+b^2$$

$$= 8[(\tfrac{2}{3}N^3+4N)^2-(\tfrac{2}{3}N^3+4N)(4N-b)]+b^2$$

$$< 8(\tfrac{2}{3}N^3+4N)^2,$$

if $4N > b$ and $N > 2$. If $N = 1$ and $4N > b$, then $b = 1,2,3$ and if $N = 2$ and $4N > b$, then $b = 1,2,\ldots,7$, and in all these cases the above inequality holds. Hence

$$\max((2x+b)^2,(2y+b)^2) < 8(\tfrac{2}{3}N^3+4N)^2$$

when $4N > b$. This implies

$$\max(|x|, |y|) < N^3$$

when $N \geq 10$ and $N > \frac{b}{4}$. The only exceptions for $N < 10$ and $b = 1,\ldots,10$ are given in the following table.

Table 3

b	N	(x,y)
1	1	(8,-10),(9,-21),(9,-6)
	2	(15,-25),(54,-12)
	4	(90,12)

b	N	(x,y)
2	1	(6,-2)
	2	(-9,-30),(16,-20),(18,-42),(18,-12),(25,-110)
	3	(30,-18),(40,-16)
	4	(108,-24)
	5	(504,-48)
	7	(648,48)
3	1	(6,-3),(9,-9)
	2	(15,-3)
	3	(-25,-135),(24,-30),(25,-45),(27,-63),(27,-18),(32,-108),(49,-315)
	7	(405,-54)
	8	(1782,-108)
	10	(2106,108)
4	2	(12,-4)
	3	(28,-4)
	4	(-49,-364),(36,-84),(50,-220),(81,-684)
5	1	(3,-1)
	2	(-14,4),(-9,3),(16,-12),(20,-30)
	3	(-96,-18),(28,-49)
	5	(-81,-765),(-32,-140),(49,-140),(72,-390),(121,-1265)
6	2	(-36,9),(12,-6),(18,-18)
	3	(-48,8)
	6	(-121,-1386),(-50,-270),(64,-216),(75,-330),(98,-630),(169,-2106)

b	N	(x,y)
7	1	(-2,3)
	3	(45,-150)
	4	(49,-147)
	7	(-169,-2275),(-72,-462),(128,-952),(225,-3255)
8	8	(-225,-3480),(-98,-728),(162,-1368),(289,-4760)
9	1	(5,-2)
	3	(27,-27)
	9	(-128,-1080),(147,-945),(200,-1890)
10	2	(15,-10)
	10	(-361,-7030),(-162,-1530),(242,-2530),(441,-9030)

In the above discussion, we have assumed that $u > 3b$. If $u = 3b$, then $x = 18b^2(4b-1)$, $y = -12b^2$ give a solution of (2) for $N = 3b-1$ and in this case we have

$$x-N^3 = 45b^3+9b(b-1)+1$$

which implies that $\max(|x|, |y|) > N^3$. Also, if $u = 3b$, then $x = 18b^2(4b+1)$, $y = 12b^2$ give a solution of (2) for $N = 3b+1$ and in this case we have

$$x-N^3 = 26b^3+(b-1)(19b^2+10b+1)$$

and consequently $\max(|x|, |y|) > N^3$.

4. THE CONSTRUCTION OF SOLUTIONS IN CASE III(d)(iii)

In this case if $u < v$ then by Lemma 2.9. We have $b < u < 4N$ and if $v < u$ then we have $0 < v < 4N$. Hence

the number of solutions in this case $\leq (4N-1)+(4N-b-1) = 8N-b-2$. Suppose $v \neq N$ and consider (38) as a quadratic equation in u. Then we have

$$(v^2+vn+2bN)^2-(N-v)^2(v+b)(v+3b) = z^2 \tag{40}$$

and

$$u = \frac{N(v^2+vN+2bN\pm z)}{(N-v)^2} \tag{41}$$

for some integer z. Rewrite (40) as

$$z^2 = 4(N-b)(v+b)^3+b^2(N-3v-2b)^2. \tag{42}$$

We consider all those values of v with $1 \leq v < 4N$, $v \neq N$ for which there is a z satisfying (42). For each such combination we determine whether u, given by (41) for one or the other sign is integral. Next suppose $u \neq N$ and consider (39) as a quadratic equation in v. Then we have

$$(u^2+uN-2bN)^2-(N-u)^2(u-b)(u-3b) = t^2 \tag{43}$$

and

$$v = \frac{N(u^2+uN-2bN\pm t)}{(N-u)^2} \tag{44}$$

for some integer t. Rewrite (43) as

$$t^2 = 4(N+b)(u-b)^3+b^2(N-3u+2b)^2. \tag{45}$$

We consider all those values of u with $1 \leq u < 4N$, $u \neq N$ for which there is a t satisfying (45). For each such combination we determine whether v, given by (44) for one or the other sign is integral.

Employing the equations (41) through (45), a program in PASCAL Language was written to find the solutions of (2) for $1 \leq b \leq 10$ and $1 \leq N \leq 100$ in Case III(d)(iii) and was run on DEC-1090 at the Computer Centre, Indian Institute of Technology, Kanpur. The program is given in an appendix at the end of this chapter. The number w given by (13), (14) and (15) has been changed to L in the program. Given $b > 0$ and $N \neq 0$, the program can be used to secure the solutions of (2) in Case III(d)(iii). The complete sets of proper non-trivial solutions of (2) for (i) $1 \leq N \leq 100$ and $1 \leq b \leq 4$ and (ii) $1 \leq N \leq 10$ and $5 \leq b \leq 10$ are given in Tables 4 through 13. No entry indicates that no such solutions exist.

Table 4(i) (R.J.Stroeker [1]). b = 1

N	(x,y)
1	(8,-10),(9,-21),(9,-6)
2	(-3,-1),(15,-25),(54,-12)
3	(-2,-1)
4	(90,12)
5	(-6,-16),(3,1),(27,6)
6	(14,4),(64,-40)
7	(-2,-3),(9,3),(50,-120)
9	(5,2)
11	(-3,-5)
13	(7,3)
15	(-9,-21),(-4,-7),(2,1),(104,-169)
17	(9,4)
18	(-25,-85),(4,2),(207,-1587),(209,-121)
19	(-5,-9)
21	(11,5)
22	(169,39)
23	(-6,-11),(867,-187)
25	(13,6)
27	(-7,-13)
29	(15,7),(125,35)
31	(-8,-15)
32	(539,-217)

N	(x,y)
33	(17,8)
34	(-70,-300)
35	(-9,-17)
37	(19,9)
38	(2883,279)
39	(-10,-19)
40	(-4,-6),(441,-273)
41	(21,10)
42	(50,20),(289,-697)
43	(-11,-21)
45	(23,11)
46	(329,-441)
47	(-12,-23)
49	(5,3),(25,12)
50	(351,-507)
51	(-247,-1805),(-36,-96),(-13,-25),(98,35),(363,-495),(494,-361)

Table 4(ii). b = 1

N	(x,y)
52	(-121,-561),(1007,-361)
53	(27,13)
55	(-14,-27)
57	(29,14)

N	(x,y)
59	(-15,-29)
61	(31,15)
63	(-16,-31)
65	(-3,-4),(33,16)
66	(-9,-15),(450,-780)
67	(-17,-33)
69	(35,17)
71	(-18,-35)
73	(37,18)
75	(-19,-37),(-6,-9),(76,32)
77	(3,2),(39,19)
79	(-20,-39)
81	(41,20)
83	(-21,-41)
85	(43,21)
87	(-36,-81),(-22,-43),(2200,-640)
89	(45,22)
91	(-23,-45)
93	(-100,-320),(47,23)
94	(1539,279)
95	(-24,-47)
97	(49,24)
99	(-25,-49),(-5,-7)
100	(909,-729)

Table 5. b = 2

N	(x,y)
1	(6,-2)
2	(-9,-30),(16,-20),(18,-42),(18,-12),(25,-110)
3	(-10,-2),(30,-18),(40,-16)
4	(-6,-2),(30,-50),(108,-24)
5	(504,-48)
6	(-4,-2),(-2,-1),(4,1)
7	(648,48)
8	(180,24)
9	(64,-112),(88,16)
10	(-12,-32),(-3,-4),(-3,-2),(6,2),(54,12),(75,-90)
11	(78,-162),(208,-72)
12	(28,8),(128,-80)
14	(-4,-6),(8,3),(18,6),(100,-240)
15	(-8,-16),(238,-98)
18	(-5,-8),(10,4)
19	(-56,-272), (168,-784)
22	(-6,-10),(12,5)
26	(-7,-12),(14,6)
30	(-18,-42),(-8,-14),(2,1),(4,2),(16,7),(208,-338)
34	(-9,-16),(18,8)
35	(222,54)
36	(-50,-170),(8,4),(414,-3174),(418,-242)

N	(x,y)
38	(-10,-18),(20,9)
42	(-275,-2420),(-11,-20),(22,10)
44	(338,78)
46	(-12,-22),(-6,-9),(24,11),(168,49),(378,-1617),(1734,-374)
50	(-13,-24),(26,12)
51	(-162,-882),(16,8)
54	(-44,-121),(-14,-26),(28,13)
57	(-72,-240)
58	(-15,-28),(30,14),(250,70)
59	(1936,264)
61	(10206,-882)
62	(-16,-30),(32,15)
64	(1078,-434)
65	(670,-450)
66	(-17,-32),(34,16)
68	(-140,-600)
70	(-18,-34),(36,17)
74	(-19,-36),(38,18)
76	(5766,558)
78	(-20,-38),(40,19)
80	(-8,-12),(882,-546)
82	(-21,-40),(42,20)
84	(100,40),(578,-1394)

N	(x,y)
85	(-42,-98),(1392,-576)
86	(-22,-42),(44,21)
89	(1800,-30000)
90	(-23,-44),(46,22)
92	(658,-882)
94	(-24,-46),(48,23)
98	(-25,-48),(10,6),(50,24)
100	(702,-1014)

Table 6. b = 3

N	(x,y)
1	(-1,1),(6,-3),(9,-9)
2	(15,-3)
3	(-25,-135),(-8,-18),(24,-30),(25,-45),(27,-63), (27,-18),(32,-108),(49,-315)
4	(-21,-3)
5	(-12,-3),(-2,-1),(81,-27)
6	(-9,-3),(-6,-4),(-3,-1),(12,2),(45,-75),(162,-36)
7	(5,1),(60,-192),(405,-54)
8	(-12,-30),(25,5),(132,-48),(1782,-108)
9	(-6,-3)
10	(-4,-2),(78,-84),(117,-63),(2106,108)
11	(-9,-18),(7,2),(24,6),(81,-108),(105,-75),(567,54)
12	(-35,-147),(-5,-3),(270,36)

N	(x,y)
13	(-4,-5),(162,27)
15	(-18,-48),(-3,-2),(3,1),(9,3),(81,18),(168,-98)
16	(162,-108)
17	(-5,-7)
18	(42,12),(192,-120)
19	(11,4)
20	(-27,-81)
21	(-6,-9),(-4,-3),(27,9),(150,-360)
22	(-45,-171)
23	(13,5)
25	(-7,-11)
27	(15,6)
29	(-68,-289),(-8,-13),(240,-975),(1152,-234)
31	(17,7),(225,-630),(459,81)
33	(-9,-15)
35	(19,8)
37	(-10,-17),(375,-255)
39	(21,9)
41	(-198,-1368),(-30,-75),(-11,-19),(81,27), (294,-399), (396,-288)
43	(23,10)
44	(4,2)
45	(-27,-63),(-12,-21),(6,3),(312,-507)
46	(-18,-36),(1617,-363)
47	(25,11)

N	(x,y)
49	(-48,-138),(-13,-23),(2,1),(429,-363)
51	(27,12)
52	(132,42)
53	(-14,-25)
54	(-75,-255),(12,6),(621,-4761),(627,-363)
55	(29,13)
57	(-15,-27)
59	(31,14)
61	(-16,-29)
63	(33,15)
65	(-147,-651),(-17,-31),(18,9),(7168,-784)
66	(49,21),(507,117)
67	(35,16)
69	(-18,-33),(-6,-8),(60,25),(2601,-561)
71	(37,17)
73	(-19,-35)
75	(39,18)
77	(-20,-37)
78	(9,5),(-36,-80)
79	(41,19)
81	(-21,-39)
83	(43,20)
85	(-22,-41)
87	(-105,-343),(-15,-25),(45,21),(375,105), (1320,242)

N	(x,y)
88	(117,45)
89	(-23,-43)
91	(47,22)
93	(-24,-45)
95	(49,23),(693,-2178)
96	(660,-1550),(1617,-651)
97	(-25,-47),(1680,294)
98	(1212,240)
99	(51,24)
100	(-507,-3783),(36,18)

Table 7. b = 4

N	(x,y)
2	(12,-4)
3	(28,-4)
4	(-49,-364),(-18,-60),(32,-40),(36,-84),(36,-24),(50,-220),(81,-684)
5	(-36,-4)
6	(-20,-4),(60,-36),(80,-32)
8	(-12,-4),(-3,-2),(6,1),(60,-100),(216,-48)
9	(416,-64)
10	(1008,-96)
11	(4320,-192)
12	(-8,-4),(-4,-2),(8,2)
13	(4896,192)
14	(1296,96)

N	(x,y)
15	(-36,-132),(380,-100),(608,64)
16	(-5,-6),(10,3),(360,48)
18	(128,-224),(176,32)
20	(-24,-64),(-6,-8),(-6,-4),(12,4),(108,24),(150,-180)
22	(156,-324),(416,-144)
24	(-7,-10),(14,5),(56,16),(256,-160)
28	(-8,-12),(-4,-3),(16,6),(36,12),(200,-480), (588,-189)
30	(-16,-32),(476,-196)
32	(-9,-14),(18,7)
36	(-10,-16),(-5,-4),(20,8)
38	(-112,-544),(336,-1568)
39	(-64,-224)
40	(-11,-18),(22,9)
44	(-12,-20),(24,10)
48	(-13,-22),(26,11)
49	(636,-324)
52	(-14,-24),(28,12)
	(3776,-544)
	(-15,-26),(30,13)
	(-36,-84), (-16,-28), (4,2),(8,4),(32,14), (100,35), (416,-676)
	(-17,-30),(34,15)
	(-18,-32),(36,16)

N	(x,y)
70	(444,108)
71	(-480,-4288)
72	(-100,-340),(-19,-34),(2,1),(16,8),(38,7), (605,-550),(828,-6348),(836,-484)
73	(576,-2208)
76	(-20,-36),(40,18)
80	(-21,-38), (42,19)
83	(-132,-484)
84	(-550,-4840),(-22,-40),(44,20)
88	(-23,-42),(46,21),(676,156)
92	(-24,-44),(-12,-18),(48,22),(336,98), (756,-3234),(3468,-748)
93	(-32,-64),(5820,-900)
96	(-25,-46),(50,23)
99	(-64,-160)
100	(-26,-48),(52,24)

Table 8. b = 5

N	(x,y)
1	(3,-1)
2	(-14,4),(-9,3),(16,-12),(20,-30)
3	(-96,-18),(-2,1),(-1,1),(20,-5),(25,-25),(28,-49)
4	(45,-5)
5	(-81,-765),(32,-140),(-9,-15),(40,-50), (45,-105),(45,-30),(49,-140),(72,-390), (121,-1265)

N	(x,y)
6	(-55,-5)
7	(-30,-5),(-3,-1)
9	(-8,-2),(-1,-2),(7,1),(70,-80),(175,-50)
10	(-15,-5),(75,-125),(270,-60)

Table 9. $b = 6$

N	(x,y)
2	(-36,9),(-6,3),(-2,2),(4,-1),(12,-6),(18,-18)
3	(-48,8),(-6,2),(18,-6),(24,-16)
4	(30,-6)
5	(48,-24),(64,-16),(66,-6)
6	(-121,-1386),(-50,-270),(-27,-90), (-16,-36), (48,-60), (50,-90),(54,-126),(54,-36), (64,-216), (75,-330), (98,-630),(169,-2106)
7	(-78,-6)
8	(-42,-6)
9	(-30,-6),(90,-54),(120,-48)
10	(-24,-6),(-18,-9),(-4,-2),(8,1),(162,-54)

Table 10. $b = 7$

N	(x,y)
1	(-2,3)
3	(5,-1),(8,-2),(45,-150)
4	(-22,-12),(33,-27),(49,-147)

N	(x,y)
5	(-27,3),(-16,2),(-3,-1),(-3, 1),(42-56), (42,-7),(48,-18)
6	(-52,-16),(-4,-2),(-1,1),(49,-49),(65,-25), (91,-7)
7	(-25,-70),(-72,-462),(-169,-2275),(56,-70), (63,-147), (63,-42),(81,-315),(128,-952),(225,-3255)
8	(-105,-7)
9	(-56,-7),(-12,-9),(-4,-1),(98,-392),(98,-49)

Table 11. b = 8

N	(x,y)
4	(-3,2),(6,-1),(24,-8)
6	(56,-8)
7	(120,-8)
8	(-225,-3480),(-98,-728),(-36,-120),(-36,-15), (64,-80),(72,-168),(72,-48),(100,-440), (100,-35), (162,-1368),(289,-4760)
9	(-136,-8)
10	(-72,-8)

Table 12. b = 9

N	(x,y)
1	(5,-2)
3	(-3,3),(18,-9),(27,-27)
5	(7,-1)

N	(x,y)
6	(45,-9)
7	(-4,1),(72,-9)
8	(-2,-4),(153,-9)
9	(-289,-5049),(-128,-1080),(-75,-405),(-75,-20),(-49,-189),(-24,-54),(-24,-14),(-3,-5),(72,-90),(75,-135),(75,-65),(81,-189),(81,-54),(96,-324),(96,-44),(121,-594),(147,-945),(147,-35),(200,-1890),(361,-6669)
10	(-171,-9),(-1,1),(81,-81)

Table 13. b = 10

N	(x,y)
2	(-3,4),(6,-2),(15,-10)
4	(-28,8),(-18,6),(32,-24),(40,-60)
5	(-30,-10)
6	(-192,-36),(-4,2),(-2,2),(8,-1),(18,-3),(40,-10),(50,-50),(50,-25),(56,-98)
8	(90,-10)
9	(190,-10)
10	(-361,-7030),(-162,-1530),(-64,-280), (-45,-150),(-18,-30), (80,-100), (90,-210), (90,-60),(98,-280),(125,-550), (144,-780), (242,-2530),(441,-9030)

REFERENCE

1. R.J.Stroeker, The Diophantine equation $(x^2+y)(x+y^2) = N(x-y)^3$, Simon Stevin, 54(1980),151-163.Zbl.446.10018.

APPENDIX

COMPUTER PROGRAM

```
PROGRAM NUMBERS ( INPUT, OUTPUT) ;

const
BLIMIT = 10 ; NLIMIT = 100 ; BLANKS = '    ' ;
var
SV,SU,B,N,V,Z,U,L,X,Y : integer ; PLUSZ, PLUSB, FLAG :
boolean ;
ICASE : 1 .. 4 ;
function FINDZ (PLUSZ,PLUSB : boolean) : integer ;
var
I,J,T,C : integer ; A : real ;
begin
if PLUSB then C : = B
else C : = -B ;
I : = 4 * (N-C) * (V+C) * (V+C) * (V+C) ;
J : = C * C *(N-3 * V - 2 * C) * (N-3 * V-2 * C);
A : = I ÷ J ;
if A > = 0 then
begin A : = SQRT(A) ;
T : = TRUNC (A) ;
if (I+J) < > T *T  then
if (I+J) < > (T+1) * (T+1) then T : = -1
else T : = T + 1 ;
```

```
end
else T : = -1;
FINDZ : = T ;
end ;
procedure FINDU (PLUSZ, PLUSB : boolean ; var U:integer
var FLAG :boolean ) ;
var
BB,ZZ,I,J : integer ; TST : real ;
begin
if PLUSZ then ZZ : = Z
else ZZ : = -Z ;
if PLUSB then BB : = B
else BB : = - B ;
I : = N *(V * V + V * N + 2 * BB * N + ZZ)
: J : = (V-N) * (V-N) ;
U : = I div J ;
if U *J < > I then FLAG : = false
else FLAG : = true ;
end ;
procedure DISPLAY (X,Y : integer) ;
const
STARS = '  ***   ' ;
begin WRITELN ;
WRITE ( BLANKS , B : 3, BLANKS, N : 4, BLANKS, V : 4,
BLANKS, Z : 8, BLANKS, U : 8 ; BLANKS, L : 8, BLANKS) ;
```

```
if ODD(X) then
if ODD(Y) then WRITELN (STARS, BLANKS, STARS)
else WRITELN ( STARS, BLANKS, ( Y div 2 ) : 8 )
else
if ODD(Y) then WRITELN ((X div 2  ) : 8, BLANKS, STARS)
else WRITELN (( X div 2 ) : 8, BLANKS, (Y div 2 ) : 8) ;
end ;
begin
WRITELN ( BLANKS, 'B', BLANKS, 'N', BLANKS, 'V',
BLANKS, 'Z', BLANKS, 'U', BLANKS, 'L', 'X'
, BLANKS, 'Y' ) ;
for ICASE : 1 to 4 do
begin
case ICASE of
1 :
begin PLUSZ : = true ; PLUSB : = true
end ;
2:
begin PLUSZ : = false ; PLUSB : = true
end ;
3:
begin PLUSZ : = true ; PLUSB : = false
end ;
4:
begin PLUSZ : = false ; PLUSB : = false
end
```

```
end ;
for B: = 1 to BLIMIT do
for N: = 1 to NLIMIT do
for V: = 1 to (4 * N-1) do
if V < > N then
begin
Z: = FINDZ (PLUSZ, PLUSB) ;
if Z > = 0 then
begin
FINDU (PLUSZ, PLUSB, U,FLAG) ;
if FLAG then
begin
L : = (U * V) div N ;
if (L * N) = (U *V) then
begin
case ICASE of
1,2 :
begin SV: = V; SU: = U
end;
3,4:
begin SV: = U, SU: = V
end

end;
X: = SV-SU +L+B; Y = SV-SU-L+B;
if (X < >0) and (Y < >0) then DISPLAY(X,Y);
```

```
end;
end;
end;
end;
end;
end,
```

CHAPTER 3

PELL'S EQUATION AND ITS APPLICATIONS

PART I : PELL'S EQUATION

1. THE DIOPHANTINE EQUATION $A^2-DB^2 = 1$

Let D be a given square-free natural number. The Diophantine equation

$$A^2 - DB^2 = 1 \qquad (1)$$

is often called the Pell's equation owing to a mistaken reference by Euler. Pell was not concerned with this equation. Actually this equation should have been designated as Fermat's equation. (see L.E. Dickson [12]). It is well known that (1) always has an infinite number of integral solutions.

LEMMA 3.1. If (A,B) is an integral solution of (1) with $D = 2$ or $D \equiv 1 \pmod 4$, then A is odd and B is even.

Proof. (1) implies $\gcd(D,A) = 1$ and $\gcd(A,B) = 1$. If $D = 2$, then A is odd and so $A^2 \equiv 1 \pmod 4$. This implies $2B^2 \equiv 0 \pmod 4$. Hence B is even. Next suppose $D \equiv 1 \pmod 4$. If A, B are both odd, then $A^2 - DB^2 \equiv 0 \pmod 4$, a contradiction. Hence one of A,B is odd and the other is even. If A is even and B is odd, then $A^2 - DB^2 \equiv 3 \pmod 4$, which is impossible. Hence A is odd and B is even. This completes the proof of Lemma 3.1.

Among all the solutions $A + B\sqrt{D}$ of the equation (1) with positive A and B, there is a least solution $A_1 + B_1\sqrt{D}$ in which A_1 and B_1 have their least values. The number $A_1 + B_1\sqrt{D}$ is called the fundamental solution of (1). All the solutions of (1) with positive A and B are obtained by the formula $A_r + B_r\sqrt{D} = (a + b\sqrt{D})^r$ where $r = 1,2,3,\ldots$ and $a + b\sqrt{D}$ is the fundamental solution of (1) i.e., $A_1 = a$ and $B_1 = b$. In [11] G.N. Copley has given the following recurrence relations for the solutions $A_r + B_r\sqrt{D}$ of (1).

$$A_{r+s} = A_r A_s + D B_r B_s \tag{2}$$

$$B_{r+s} = A_r B_s + B_r A_s \tag{3}$$

$$A_{r+1} = A_1 A_r + D B_1 B_r \tag{4}$$

$$B_{r+1} = A_1 B_r + B_1 A_r \tag{5}$$

$$A_{2r} = 2A_r^2 - 1 \tag{6}$$

$$B_{2r} = 2A_r B_r \tag{7}$$

$$A_{3r} = A_r (4A_r^2 - 3) \tag{8}$$

$$B_{3r} = B_r (4A_r^2 - 1) \tag{9}$$

For the solutions of (1) we also have the following relations :

$$A_{5r} = A_r (16A_r^4 - 20A_r^2 + 5) \tag{10}$$

$$B_{5r} = B_r (16A_r^4 - 12A_r^2 + 1) \tag{11}$$

$$A_{15r} = A_r(4A_r^2-3)(16A_r^4-20A_r^2+5) \times$$
$$(256A_r^8 - 448A_r^6 + 224A_r^4 - 32A_r^2 + 1) \tag{12}$$

$$B_{15r} = B_r(4A_r^2 - 1)\ (16A_r^4 - 12A_r^2 + 1) \times$$
$$(256A_r^8 - 576A_r^6 + 416A_r^4 - 96A_r^2 + 1) \tag{13}$$

$$A_{-r} = A_r \tag{14}$$

$$B_{-r} = -B_r \tag{15}$$

E.I. Emerson [13] gave the relations

$$A_{r+2} = 2a\ A_{r+1} - A_r \tag{16}$$

$$B_{r+2} = 2a\ B_{r+1} - B_r. \tag{17}$$

Pell's equation with restrictions has been studied by A. Baker and H. Davenport [4], J.H.E. Cohn [6-10], P. Kanagasabapathy and Tharmambikai Ponnudurai [17], Tharmambikai Ponnudurai [22] and Manoranjitham Veluppillai [23]. Most of the times the restriction happens to be the requirement that a function of A_r or B_r be a square. From (6), it follows that $\frac{A_{2r}+1}{2}$ is always a square. Rewriting (6) as $A_{2r} = 2D\ B_r^2 + 1$, we see that $\frac{A_{2r}-1}{2D}$ is also a square. Further, if $D = 2$, then $A_{2r}-1$ is also a square. A similar result is provided by

THEOREM 3.2. The following are always perfect squares :

(i). $\frac{A_{2r+1}-1}{\beta}$, if $a-1 = \alpha^2\beta$ with β square-free

(ii). $\frac{A_{2r+1}+1}{\delta}$, if $a+1 = \gamma^2\delta$ with δ square-free.

Proof. Using (4) we have

$$A_{2r+1} = a\ A_{2r} + b\ D\ B_{2r}.$$

Using (6) and (7), we get

$$A_{2r+1} = 2a\ A_r^2 + 2b\ D\ A_r\ B_r - a.$$

Hence

$$A_{2r+1}-1 = 2a\ A_r^2 + 2bDA_rB_r-(a+1)\ (A_r^2-DB_r^2)$$

$$= (a-1)\ A_r^2 + 2bDA_rB_r+(a+1)D\ B_r^2.$$

Similarly we have

$$A_{2r+1}+1 = (a+1)A_r^2+2bDA_rB_r+(a-1)D\ B_r^2.$$

Now

(i). Let $a-1 = \alpha^2\beta$ where α,β are integers and β is square-free. Then from $a^2-Db^2 = 1$, we have

$$\alpha^2\beta\ (\alpha^2\beta + 2) = Db^2.$$

This implies $\alpha^2\beta|Db^2$. Let

$$\alpha = p_1^{i_1}\ p_2^{i_2}\ \cdots\ p_k^{i_k}$$

and

$$\beta = p_{s_1}\ p_{s_2}\ \cdots\ p_{s_t}\ q_1\ q_2\ \cdots\ q_m$$

be the prime factorizations of α and β respectively, where $\{p_{s_1},\ldots,p_{s_k}\} \subseteq \{p_1,\ldots,p_k\}$. Then

$$\alpha^2\beta = p_1^{j_1}\ p_2^{j_2}\ \cdots\ p_k^{j_k}\quad q_1q_2\cdots q_m|Db^2$$

where $j_n = 2i_n+1$ or $2i_n$ $(1 \le n \le k)$. First suppose $j_n = 2i_n+1$. If $p_n | D$, then $p_n^{2i_n} | b^2$. i.e., $p_n^{i_n} | b$. So $p_n^{i_n+1} | bD$. If $p_n \nmid D$, then $p_n^{2i_n+1} | b^2$. i.e., $p_n^{i_n+1} | b$. Thus in any case $p_n^{i_n+1} | bD$. Next suppose $j_n = 2i_n$. Then $p_n \nmid D$ and $p_n^{i_n} | b$. So $p_n^{i_n} | bD$. Clearly $q_1, \ldots, q_m$ each $|$ bd. Hence $\alpha\beta | bD$. Thus $\frac{bD}{\alpha\beta}$ is an integer. Now

$$\frac{A_{2r+1}-1}{\beta} = \alpha^2 A_r^2 + \frac{2bD}{\beta} A_r B_r + \frac{\alpha^2 \beta+2}{\beta} DB_r^2 = (\alpha A_r + \frac{bD}{\alpha\beta} B_r)^2.$$

(ii). Let $a+1 = \gamma^2\delta$ where δ is square-free. As before we can see that $\frac{bD}{\gamma\delta}$ is an integer and

$$\frac{A_{2r+1}+1}{\delta} = (\gamma A_r + \frac{bD}{\gamma\delta} B_r)^2.$$

This completes the proof of Theorem 3.2.

2. THE DIOPHANTINE EQUATION $U^2-DV^2=N$

Now we consider the general Pell's equation

$$U^2 - DV^2 = N \tag{18}$$

where N is a given non-zero integer. We assume the solvability of (18). If $U + V\sqrt{D}$ and $U' + V'\sqrt{D}$ are both solutions to (18) then they are called associate solutions if and only if there exists a solution $A + B\sqrt{D}$ to $A^2-DB^2 = 1$ such that

$$U + V\sqrt{D} = (U'+V'\sqrt{D})\ (A + B\sqrt{D}).$$

The set of all solutions associated with each other forms a class of solutions of (18). Every class contains an infinite number of solutions. (see e.g. Nagell [21]).

THEOREM 3.3. (Nagell [21]). If $U + V\sqrt{D}$ and $U' + V'\sqrt{D}$ are two solutions of (18), a necessary and sufficient condition for these two solutions to belong to the same class is that the two numbers

$$\frac{UU' - VV'D}{N} \quad \text{and} \quad \frac{VU' - UV'}{N}$$

are integers.

If K is the class consisting of the solutions $U_r+V_r\sqrt{D}$, $r = 1,2,3,\ldots$, it is clear that the solutions $U_r-V_r\sqrt{D}$, $r = 1,2,3,\ldots$, also constitute a class, which may be denoted by $\bar{K}$. The classes K and $\bar{K}$ are said to be conjugates of each other. Conjugate classes are in general distinct, but may sometimes coincide; in the latter case we speak of ambiguous classes.

We consider a class K of solutions of (18) and fix it. Among all the solutions $U + V\sqrt{D}$ in K we now choose a solution $U^* + V^*\sqrt{D}$ as follows : Let V^* be the least non-negative value of V which occurs in K. If K is not ambiguous, then the number U^* is also uniquely determined; for the solution $-U^* + V^*\sqrt{D}$ belongs to the conjugate class $\bar{K}$. If K is ambiguous, we get a uniquely determined U^* by prescribing that $U^* \geq 0$. The solution $U^* + V^*\sqrt{D}$ defined in this way is said to be the fundamental solution of the class. In the fundamental solution the number $|U^*|$ has the least value which is possible for $|U|$ when $u+v\sqrt{D}$ belongs to K. The case $U^* = 0$ can occur only when the class is ambiguous, and similarly for the case $V^* = 0$. If $N = \pm 1$, clearly there is only one class, and then it is ambiguous.

Let $u + v\sqrt{D}$ be the fundamental solution of(18) in K.

THEOREM 3.4. (Nagell [21]). If N is positive, then

$$0 < |u| \leq \sqrt{\frac{1}{2}(a+1)N}$$

and

$$0 \leq v \leq \frac{b}{\sqrt{2(a+1)}}\sqrt{N}$$

and if $N = -N_1$ where N_1 is positive, then

$$0 \leq |u| \leq \sqrt{\frac{1}{2}(a-1)N_1}$$

and

$$0 < v \leq \frac{b}{\sqrt{2(a-1)}}\sqrt{N_1}.$$

Let $U_r + V_r\sqrt{D}$ $(r = 0,1,2,\ldots)$ be the solutions of (18) contained in K. Then we have

$$U_r + V_r\sqrt{D} = (u + v\sqrt{D})\,(a+b\sqrt{D})^r$$

where $a+b\sqrt{D}$ is the fundamental solution of (1).

LEMMA 3.5.

$$U_r = u\,A_r + Dv\,B_r \tag{19}$$

$$V_r = v\,A_r + u\,B_r \tag{20}$$

Proof.

$$U_r+V_r\sqrt{D} = (u+v\sqrt{D})\,(a+b\sqrt{D})^r = (u+v\sqrt{D})(A_r+B_r\sqrt{D})$$

$$= uA_r + DvB_r + (v\,A_r + u\,B_r)\sqrt{D}.$$

LEMMA 3.6.

$$U_{-r} = u\,A_r - Dv\,B_r \tag{21}$$

$$V_{-r} = v\, A_r - u\, B_r \tag{22}$$

Proof. Follows from (19), (20), (14) and (15).

LEMMA 3.7.

$$U_{r+s} = A_s\, U_r + D\, B_s\, V_r \tag{23}$$

$$V_{r+s} = B_s\, U_r + A_s\, V_r \tag{24}$$

Proof. $U_{r+s} + V_{r+s}\sqrt{D} = (u+v\sqrt{D})\ (a+b\sqrt{D})^{r+s}$

$$= ((u+v\sqrt{D})\quad (a+b\sqrt{D})^{r} \quad (a+b\sqrt{D})^{s}$$

$$= (U_r + V_r\sqrt{D})\quad (A_s + B_s\sqrt{D})$$

$$= (A_s\, U_r + D\, B_s V_r) + (B_s\, U_r + A_s\, V_r)\sqrt{D}.$$

LEMMA 3.8.

$N \mid u\, U_r - D\, v\, V_r$, $N \mid u\, V_r - v\, U_r$,

$$\frac{u\, U_r - D\, v\, V_r}{N} = A_r, \tag{25}$$

$$\frac{u\, V_r - v\, U_r}{N} = B_r. \tag{26}$$

Proof. Applying Cramer's rule to (19) and (20), we have

$$A_r \begin{vmatrix} u & Dv \\ v & u \end{vmatrix} = \begin{vmatrix} U_r & Dv \\ V_r & u \end{vmatrix}$$

i.e. $A_r\, N = u\, U_r - D\, v\, V_r$.

Hence $N \mid u\, U_r - D\, v\, V_r$ and (25) holds. (26) follows similarly.

LEMMA 3.9.

$$U_{r+s} = \frac{u\,U_s - D\,v\,V_s}{N}\,U_r + D\,\frac{(uV_s - v\,U_s)}{N}\,V_r \tag{27}$$

$$V_{r+s} = \frac{uV_s - v\,U_s}{N}\,U_r + \frac{u\,U_s - D\,v\,V_s}{N}\,V_r \tag{28}$$

Proof. Follows from Lemmas 3.7 and 3.8.

LEMMA 3.10. $N \mid (u^2+Dv^2)U_r - 2DuvV_r$, $N \mid 2uvU_r - (u^2+Dv^2)V_r$,

$$U_{-r} = \frac{1}{N}\{(u^2 + Dv^2)\,U_r - 2Duv\,V_r\}, \tag{29}$$

$$V_{-r} = \frac{1}{N}\{2uv\,U_r - (u^2+Dv^2)V_r\} \tag{30}$$

Proof. Follows from Lemmas 3.6 and 3.8.

LEMMA 3.11.

$$U_{r+2} = 2a\,U_{r+1} - U_r \tag{31}$$

$$V_{r+2} = 2a\,V_{r+1} - V_r \tag{32}$$

Proof. From (23), we get

$$U_{r+1} = a\,U_r + bD\,V_r. \tag{33}$$

Using (33), (23) and (24), we get

$$U_{r+2} = a(a\,U_r + bDV_r) + bD(bU_r + a\,V_r)$$

$$= (a^2+Db^2)\,U_r + 2ab\,D\,V_r. \tag{34}$$

From (34) and (33) we obtain

$$U_{r+2} - 2a\,U_{r+1} = -(a^2 - Db^2)\,U_r = -U_r.$$

Hence (31) follows. Similarly, using $V_{r+1} = bU_r + a V_r$ and $V_{r+2} = 2ab\, U_r + (a^2 + Db^2) V_r$, we get (32).

From (16), (17), (31) and (32) we have the following

LEMMA 3.12. $\{A_r\}$, $\{B_r\}$, $\{U_r\}$ and $\{V_r\}$ have the same recurrence relation.

LEMMA 3.13.

$$U_{r+2s} = -U_r + 2A_s^2 U_r + 2DA_s B_s V_r \tag{35}$$

$$= U_r + 2DB_s^2 U_r + 2DA_s B_s V_r \tag{36}$$

$$V_{r+2s} = 2A_s B_s U_r + 2A_s^2 V_r - V_r \tag{37}$$

$$= 2A_s B_s U_r + 2D B_s^2 V_r + V_r \tag{38}$$

Proof. From (23), we obtain

$$U_{r+2s} = A_{2s} U_r + D B_{2s} V_r .$$

Using (6) and (7), we get (35). Using $A_{2s} = 2DB_s^2 + 1$ and (7), we get (36). (37) and (38) follow similarly.

COROLLARY 3.14.

$$U_{r+2s} \equiv -U_r \pmod{A_s} \tag{39}$$

$$\equiv U_r \pmod{B_s} \tag{40}$$

$$V_{r+2s} \equiv -V_r \pmod{A_s} \tag{41}$$

$$\equiv V_r \pmod{B_s} \tag{42}$$

Similary we have

$$A_{r+2s} \equiv -A_r \pmod{A_s} \qquad (39)'$$

$$\equiv A_r \pmod{B_s} \qquad (40)'$$

$$B_{r+2s} \equiv - B_r \pmod{A_s} \qquad (41)'$$

$$\equiv B_r \pmod{B_s}. \qquad (42)'$$

DEFINITION 3.1. Let t be a natural number. We define

$$a_t = A_{2^{t-1}}, \qquad (43)$$

$$b_t = B_{2^{t-1}}. \qquad (44)$$

The values of a_t and b_t for $t = 1,2,3,4$ are given in the following table.

t	a_t	b_t
1	a	b
2	$2a^2-1$	$2ab$
3	$8a^4-8a^2+1$	$4ab(2a^2-1)$
4	$128a^8-256a^6+160a^4-32a^2+1$	$8ab(2a^2-1)(8a^4-8a^2+1)$

Table 1

Using the relations (6) and (7), by induction we obtain the following :

$$a_t \equiv 1 \pmod 4, \text{ for all } t \geq 3 \qquad (45)$$

$$b_t \equiv 0 \pmod 4, \text{ for all } t \geq 3 \qquad (46)$$

$$a_t \equiv 1 \pmod 8, \quad \text{for all } t \geq 3 \tag{47}$$

$$b_t \equiv 0 \pmod 8, \quad \text{for all } t \geq 4. \tag{48}$$

LEMMA 3.15.

$$\text{(i)} \quad \left(\frac{-1}{a_t^2 + Db_t^2}\right) = \begin{cases} -1 & \text{if } D \equiv 3 \pmod 4,\ t = 1, \text{ and } a \text{ is even} \\ +1, & \text{otherwise} \end{cases} \tag{49}$$

$$\text{(ii)} \quad \left(\frac{D}{a_t^2 + Db_t^2}\right) = \begin{cases} -1 & \text{if } D \equiv 3 \pmod 4, t = 1 \text{ and } a \text{ is even} \\ +1, & \text{otherwise} \end{cases} \tag{50}$$

where $(\frac{a}{b})$ denotes the Jacobi symbol.

Proof. If $D \equiv 3 \pmod 4$, $t = 1$ and a is even, then b is odd and $a^2+Db^2 \equiv 3 \pmod 4$. So $\left(\frac{-1}{a_t^2 + Db_t^2}\right) = -1$. In all the other cases, a_t is odd and b_t is even and hence $a_t^2 + Db_t^2 \equiv 1 \pmod 4$. Therefore $\left(\frac{-1}{a_t^2 + Db_t^2}\right) = +1$. Thus (49) holds.

Next we prove that (50) holds. When $D = 2$, $a_t^2 + Db_t^2 \equiv 1 \pmod 8$. So $\left(\frac{D}{a_t^2 + Db_t^2}\right) = +1$. If $D \equiv 3 \pmod 4$, $t = 1$ and a is even, then $a^2 + Db^2 \equiv 3 \pmod 4$. Noting that $\gcd(D, a^2+Db^2)=1$, we have

$$\left(\frac{D}{a_t^2+Db_t^2}\right) = \left(\frac{D}{a^2+Db^2}\right) = -\left(\frac{a^2+Db^2}{D}\right) = -\left(\frac{a^2}{D}\right) = -1.$$

Now consider $D \equiv 1 \pmod 4$, $t \geq 1$ or $D \equiv 3 \pmod 4$, $t \geq 1$, a odd or $D \equiv 3 \pmod 4$, $t \geq 2$, a even. In all these cases, $a_t^2 + Db_t^2 \equiv 1 \pmod 4$. Also we have $\gcd(D, a_t^2 + Db_t^2) = 1$. Hence

$$\left(\frac{D}{a_t^2 + Db_t^2}\right) = \left(\frac{a_t^2 + Db_t^2}{D}\right) = \left(\frac{a_t^2}{D}\right) = +1.$$

Therefore (50) holds.

COROLLARY 3.16. $\left(\frac{-D}{a_t^2 + Db_t^2}\right) = +1$ for all $t \geq 1$.

Now we discuss the method of establishing the impossibility of a non-negative integer n such that $n \equiv i \pmod{m}, n \neq i$, $0 \leq i < m$ and $U = U_n$ satisfies the simultaneous equations

$$\left.\begin{aligned} U^2 - DV^2 &= N, \\ Z^2 - gU^2 &= h \end{aligned}\right\} \qquad (51)$$

where g,h are given integers and m is 6, 10 or 30, or a multiple of them by a power of 2.

First let m be 6 or a multiple of 6 by a power of 2. Write $n = i + 3.2^t (2\lambda+1)$ where λ is a non-negative integer and t is an appropriately chosen natural number. For example, if m = 6, then $t \geq 1$; if m = 12, then $t \geq 2$; if m = 24, then $t \geq 3$, etc. Denote 2^t by k. Then $n = 3k + i + 6(\lambda-1)k+2(3k)$. Using (39), we have

$$U_n \equiv - U_{3k+i+6(\lambda-1)k} \pmod{A_{3k}}.$$

Successively using (39), we get

$$U_n \equiv (-1)^{\lambda} U_{3k+i} \pmod{A_{3k}}.$$

Using (23), we obtain

$$U_n \equiv (-1)^{\lambda} DV_i B_{3k} \pmod{A_{3k}}.$$

Hence $Z^2 \equiv g\,D^2\,V_i^2\,B_{3k}^2 + h \pmod{A_{3k}}$.

i.e.,

$$Z^2 \equiv gD^2\,V_i^2\,b_{t+1}^2\,(4a_{t+1}^2 - 1)^2 + h \pmod{a_{r+1}(4a_{t+1}^2-3)}. \tag{52}$$

Considering (52) modulo a_{t+1}, we have

$$Z^2 \equiv gD^2\,V_i^2\,b_{t+1}^2 + h \pmod{a_{t+1}}. \tag{53}$$

We use $a_{t+1} = a_t^2 + Db_t^2$, $b_{t+1} = 2a_t\,b_t$ and $1 = a_t^2-Db_t^2 \equiv -2Db_t^2$ $(\mathrm{mod}\ a_t^2 + Db_t^2)$. We obtain

$$Z^2 \equiv 2D(2gDV_i^2a_t^2-h)b_t^2 \pmod{a_t^2 + Db_t^2}.$$

Now $2gDV_i^2a_t^2-h = 2gDV_i^2(a_t^2+Db_t^2)-2gD^2V_i^2b_t^2-h \equiv -2D(gDV_i^2-h)b_t^2$

$(\mathrm{mod}\ a_t^2 + Db_t^2)$.

Hence $Z^2 \equiv -4D^2(gDV_i^2 - h)b_t^4 \pmod{a_t^2 + Db_t^2}$. Consequently we have

$$\left(\frac{-4D^2(gDV_i^2-h)b_t^4}{a_t^2 + Db_t^2}\right) = \left(\frac{-1}{a_t^2 + Db_t^2}\right)\left(\frac{gDV_i^2 - h}{a_t^2 + Db_t^2}\right)$$

where $(\frac{a}{b})$ denotes the Jacobi symbol.

Next we consider (52) modulo $4a_{t+1}^2-3$. Since $4a_{t+1}^2 - 3 = 4Db_{t+1}^2 + 1$, we have

$$Z^2 \equiv 4gD^2V_i^2\,b_{t+1}^2 + h \pmod{4Db_{t+1}^2 + 1}. \tag{54}$$

Now $4gD^2V_i^2\,b_{t+1}^2 = gDV_i^2\,(4Db_{t+1}^2+1)-gDV_i^2 \equiv -gDV_i^2 \pmod{4Db_{t+1}^2+1}$.

Hence $Z^2 \equiv -(gDV_i^2 - h) \pmod{4Db_{t+1}^2 + 1}$.

Now $\left(\frac{-(gDV_i^2 - h)}{4D\, b_{t+1}^2 + 1}\right) = \left(\frac{-1}{4Db_{t+1}^2+1}\right) \left(\frac{gDV_i^2 - h}{4Db_{t+1}^2+1}\right) = \left(\frac{gDV_i^2 - h}{4Db_{t+1}^2+1}\right)$.

Next let m be 10 or a multiple of 10 by a power of 2. Then $n = i + 5.2^t(2\lambda+1)$. With the above notations, we have $U_n \equiv (-1)^\lambda D V_i B_{5k} \pmod{A_{5k}}$ and

$$Z^2 \equiv gD^2 V_i^2 b_{t+1}^2 (16a_{t+1}^4 - 12a_{t+1}^2 + 1)^2 + h$$

$$\pmod{a_{t+1}(16a_{t+1}^4 - 20a_{t+1}^2 + 5)}. \qquad (52(a))$$

Considering (52(a)) modulo a_{t+1}, we are led to (53). Next we consider (52(a)) modulo $16a_{t+1}^4 - 20a_{t+1}^2 + 5 = 16D^2b_{t+1}^4+12Db_{t+1}^2+1$. We obtain

$$Z^2 \equiv 16gD^2 V_i^2 b_{t+1}^2 (2Db_{t+1}^2 + 1)^2 + h \qquad (55)$$

$$\equiv 4gD^2 V_i^2 b_{t+1}^2 (4Db_{t+1}^2 + 3) + h$$

$$\equiv -(gDV_i^2-h) \pmod{16D^2b_{t+1}^4+12Db_{t+1}^2+1}.$$

We have

$$\left(\frac{-(gDV_i^2-h)}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right) = \left(\frac{gDV_i^2 - h}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right).$$

Next let m be 30 or a multiple of 30 by a power of 2. Then $n = i + 15.2^t(2\lambda+1)$. With the same notations as above, we have $U_n \equiv (-1)^\lambda DV_i B_{15k} \pmod{A_{15k}}$ and

$$Z^2 \equiv gD^2V_i^2b_{t+1}^2(4a_{t+1}^2-1)^2(16a_{t+1}^4-12a_{t+1}^2+1)^2 \times$$

$$(256a_{t+1}^8-576a_{t+1}^6+416a_{t+1}^4-96a_{t+1}^2+1)^2 + h$$

$$(\text{mod } a_{t+1}(4a_{t+1}^2-3)(16a_{t+1}^4-20a_{t+1}^2+5)(256a_{t+1}^8-448a_{t+1}^6$$

$$+ 224a_{t+1}^4 - 32a_{t+1}^2+1)). \quad (52(b))$$

Considering (52(b)) modulo a_{t+1}, $4a_{t+1}^2-3$ and $16a_{t+1}^4-20a_{t+1}^2+5$, we arrive at (53), (54) and (55) respectively. Now we consider (52(b)) modulo

$$256a_{t+1}^8-448a_{t+1}^6+224a_{t+1}^4-32a_{t+1}^2 + 1$$

$$= 256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1.$$

We obtain

$$Z^2 \equiv gD^2V_i^2b_{t+1}^2(4Db_{t+1}^2+3)^2(16D^2b_{t+1}^4+20Db_{t+1}^2+5)^2 \times$$

$$(256D^4b_{t+1}^8+448D^3b_{t+1}^6+224D^2b_{t+1}^4+32Db_{t+1}^2+1)^2 + h$$

$$\equiv gD^2V_i^2b_{t+1}^2(4Db_{t+1}^2+3)^2(16D^2b_{t+1}^4+20Db_{t+1}^2+5)^2 \times$$

$$(128D^3b_{t+1}^6 + 192D^2b_{t+1}^4+64Db_{t+1}^2)^2 + h$$

$$\equiv 4gD^2V_i^2b_{t+1}^2(16D^2b_{t+1}^4+20Db_{t+1}^2+5)^2 + h$$

$$\equiv -(gDV_i^2-h)(\text{mod } 256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1).$$

We have

$$\left(\frac{-(gDV_i^2 - h)}{256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1}\right)$$

$$= \left(\frac{gDV_i^2 - h}{256D^4b_{t+1}^8 + 576D^3b_{t+1}^6 + 416D^2b_{t+1}^4 + 96Db_{t+1}^2 + 1}\right).$$

Thus we have to factorize $gDV_i^2 - h$ into primes and find the values of t for which at least one of $\left(\frac{-1}{a_t^2 + Db_t^2}\right)\left(\frac{gDV_i^2 - h}{a_t^2 + Db_t^2}\right)$, $\left(\frac{gDV_i^2 - h}{4Db_{t+1}^2 + 1}\right)$, $\left(\frac{gDV_i^2 - h}{16D^2b_{t+1}^4 + 12Db_{t+1}^2 + 1}\right)$,

$$\left(\frac{gDV_i^2 - h}{256D^4b_{t+1}^8 + 576D^3b_{t+1}^6 + 416D^2b_{t+1}^4 + 96Db_{t+1}^2 + 1}\right) \text{ is } -1.$$

DEFINITION 3.2. Since the number $gDV_i^2 - h$ plays a fundamental role, we call it the characteristic number of the system (51) for given i.

In view of what we observed in several problems, it is to be remarked that the quadratic reciprocity method does not always lead to decisive results.

Next we discuss the method of establishing the impossibility of a non-negative integer n such that $n \equiv i \pmod{m}$, $n \neq i$, $0 \leq i < m$ and $V = V_n$ satisfies the simultaneous equations

$$\left.\begin{aligned} U^2 - DV^2 &= N, \\ Z^2 - gV^2 &= h \end{aligned}\right\} \qquad (56)$$

where g, h are given integers and m is 6, 10 or 30, or a multiple of them by a power of 2.

First let m be 6 or a multiple of 6 by a power of 2.

Write $n = i + 3.2^t (2\lambda+1)$ where λ, t are as in the preceding discussion. Denote 2^t by k. Using (41), we have

$$V_n \equiv -V_{3k+i+6(\lambda-1)k} \pmod{A_{3k}}.$$

Successively using (41), we get

$$V_n \equiv (-1)^\lambda V_{3k+i} \pmod{A_{3k}}.$$

Using (24), we obtain

$$V_n \equiv (-1)^\lambda U_i B_{3k} \pmod{A_{3k}}.$$

Hence $Z^2 \equiv gU_i^2 B_{3k}^2 + h \pmod{A_{3k}}$.

i.e.,

$$Z^2 \equiv gU_i^2 b_{t+1}^2 (4a_{t+1}^2 - 1)^2 + h \pmod{a_{t+1}(4a_{t+1}^2-3)}. \tag{57}$$

Considering (57) modulo a_{t+1}, we have

$$Z^2 \equiv gU_i^2 b_{t+1}^2 + h \pmod{a_{t+1}} \tag{58}$$

$$\equiv 2(2gU_i^2a_t^2 - Dh)b_t^2 \pmod{a_t^2 + Db_t^2}$$

$$\equiv -4D(gU_i^2 - Dh)b_t^4 \pmod{a_t^2 + Db_t^2}.$$

Now

$$\left(\frac{-4D(gU_i^2 - Dh)b_t^4}{a_t^2+Db_t^2}\right) = \left(\frac{-D}{a_t^2+Db_t^2}\right)\left(\frac{gU_i^2 - Dh}{a_t^2 + Db_t^2}\right) = \left(\frac{gU_i^2 - Dh}{a_t^2 + Db_t^2}\right),$$

using Corollary 3.16.

Next, considering (57) modulo $4a_{t+1}^2-3$, we obtain

$$Z^2 \equiv 4gU_i^2b_{t+1}^2 + h \pmod{4Db_{t+1}^2 + 1}. \tag{59}$$

We have

$$\left(\frac{4gU_i^2b_{t+1}^2+h}{4Db_{t+1}^2+1}\right) = \left(\frac{D}{4Db_{t+1}^2+1}\right)\left(\frac{gU_i^2(4Db_{t+1}^2+1)-gU_i^2+Dh}{4Db_{t+1}^2+1}\right)$$

$$= \left(\frac{-1}{4Db_{t+1}^2+1}\right)\left(\frac{D}{4Db_{t+1}^2+1}\right)\left(\frac{gU_i^2 - Dh}{4Db_{t+1}^2+1}\right).$$

Clearly $\left(\frac{-1}{4Db_{t+1}^2+1}\right) = +1$. If $D = 2$, then

$$4Db_{t+1}^2 + 1 \equiv 1 \pmod 8 \text{ and so } \left(\frac{D}{4Db_{t+1}^2+1}\right) = +1.$$

If D is odd, then $\left(\frac{D}{4Db_{t+1}^2+1}\right) = \left(\frac{4Db_{t+1}^2+1}{D}\right) = \left(\frac{1}{D}\right) = +1.$

Thus in any case we obtain $\left(\frac{D}{4Db_{t+1}^2+1}\right) = +1$. Hence

$$\left(\frac{4gU_i^2b_{t+1}^2+h}{4Db_{t+1}^2+1}\right) = \left(\frac{gU_i^2 - Dh}{4Db_{t+1}^2+1}\right).$$

Next let m be 10 or a multiple of 10 by a power of 2. Then $n = i + 5.2^t(2\lambda+1)$. We have $V_n \equiv (-1)^\lambda U_i B_{5k} \pmod{A_{5k}}$ and

$$z^2 \equiv gU_i^2b_{t+1}^2(16a_{t+1}^4 - 12a_{t+1}^2 + 1)^2 + h$$
$$\pmod{a_{t+1}(16a_{t+1}^4 - 20a_{t+1}^2 + 5)}. \qquad (57(a))$$

Considering (57(a)) modulo a_{t+1}, we are led to (58). Next we consider (57(a)) modulo $16a_{t+1}^4 - 20a_{t+1}^2 + 5$. We get

$$Z^2 \equiv 16g\,U_i^2\,b_{t+1}^2\,(2Db_{t+1}^2+1)^2+h$$

$$\pmod{16D^2b_{t+1}^4+12Db_{t+1}+1} \tag{60}$$

$$\equiv 4gU_i^2\,b_{t+1}^2\,(4Db_{t+1}^2+3)+h.$$

W

$$\left(\frac{4gU_i^2\,b_{t+1}^2\,(4Db_{t+1}^2+3)+h}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right)$$

$$=\left(\frac{D}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right)\left(\frac{-gU_i^2+Dh}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right)$$

$$=\left(\frac{gU_i^2-Dh}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right),\ \text{since}\ \left(\frac{-1}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right)=+1$$

and $\left(\frac{D}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right)=+1.$

Next let m be 30 or a multiple of 30 by a power of 2. Then $n = i + 15\cdot 2^t\,(2\lambda+1)$. We get

$$V_n \equiv (-1)^\lambda\,U_i\,B_{15k} \pmod{A_{15k}}\ \text{and}$$

$$Z^2 \equiv gU_i^2b_{t+1}^2(4a_{t+1}^2-1)^2\,(16a_{t+1}^4-12a_{t+1}^2+1)^2\,\times$$

$$(256a_{t+1}^8-576a_{t+1}^6+416a_{t+1}^4-96a_{t+1}^2+1)^2+h$$

$$(\mathrm{mod}\ a_{t+1}(4a_{t+1}^2-3)(16a_{t+1}^4-20\,a_{t+1}^2+5)\,\times$$

$$(256a_{t+1}^8-448a_{t+1}^6+224a_{t+1}^4-32\,a_{t+1}^2+1)). \tag{57(b)}$$

Considering (57(b)) modulo a_{t+1}, $4a_{t+1}^2-3$ and $16a_{t+1}^4-20a_{t+1}^2+5$,

we are led to (58), (59) and (60) respectively. Now we consider (57(b)) modulo $256a_{t+1}^8-448a_{t+1}^6+224a_{t+1}^4-32a_{t+1}^2+1$ and obtain

$$Z^2 \equiv gU_i^2b_{t+1}^2(4Db_{t+1}^2+3)^2\ (16D^2b_{t+1}^4+20Db_{t+1}^2+5)^2 \times$$
$$(256D^4b_{t+1}^8+448D^3b_{t+1}^6+224D^2b_{t+1}^4+32Db_{t+1}^2+1)^2 + h$$
$$\equiv 4gU_i^2b_{t+1}^2(16D^2b_{t+1}^4+20Db_{t+1}^2 + 5)^2 + h$$
$$(\mathrm{mod}\ 256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1).$$

Now

$$\left(\frac{4gU_i^2b_{t+1}^2(16D^2b_{t+1}^4+20Db_{t+1}^2+5)^2 + h}{256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1}\right)$$

$$= \left(\frac{D}{256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1}\right) \times$$

$$\left(\frac{-gU_i^2 + Dh}{256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1}\right)$$

$$= \left(\frac{gU_i^2 - Dh}{256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1}\right).$$

Thus we have to factorize $gU_i^2 - Dh$ into primes and find the values of t for which at least one of $\left(\frac{gU_i^2 - Dh}{a_t^2 + Db_t^2}\right)$, $\left(\frac{gU_i^2-Dh}{4Db_{t+1}^2+1}\right)$, $\left(\frac{gU_i^2 - Dh}{16D^2b_{t+1}^4+12Db_{t+1}^2+1}\right)$, $\left(\frac{gU_i^2 - Dh}{256D^4b_{t+1}^8+576D^3b_{t+1}^6+416D^2b_{t+1}^4+96Db_{t+1}^2+1}\right)$ is -1.

DEFINITION 3.3. Since the number $gU_i^2 - Dh$ plays a fundamental role, we call it the characteristic number of the system (56) for given i.

PART II : APPLICATIONS OF PELL'S EQUATION

We now consider some applications of Pell's equation.

3. THE DIOPHANTINE EQUATION

$$Y(Y+1)(Y+2)(Y+3) = 3X(X+1)(X+2)(X+3).$$

In [22] Tharmambikai Ponnudurai has proved that the only solutions in positive integers of the Diophantine equation

$$Y(Y+1)(Y+2)(Y+3) = 3X(X+1)(X+2)(X+3) \tag{61}$$

are $X = 2$, $Y = 3$ and $X = 5$, $Y = 7$. She had to solve the Diophantine equation

$$U^2 - 3V^2 = -2 \tag{62}$$

with the restrictions given by

$$y^2 = 5 + 4U_n \tag{63}$$

$$x^2 = 5 + 4V_n \tag{64}$$

where $U_n + \sqrt{3}\, V_n$ is a solution of (62). For this purpose she introduced two functions η_r and ξ_r in terms of α and β where $\alpha = 1 + \sqrt{3}$ and $\beta = 1 - \sqrt{3}$. The method used is quadratic reciprocity. The congruences are taken modulo $\eta_r 2^{-s}$ where $0 \leq s \leq r$.

We find that the method becomes complicated by the introduction η_r and ξ_r. We indicate here that η_r and ξ_r

can be dispensed with and the problem can be handled quite easily.

The Pell's equation

$$A^2 - 3B^2 = 1 \tag{65}$$

has the fundamental solution $A_1 = 2$, $B_1 = 1$. The equation (62) has only one class of solutions and the solutions are given by

$$U_r + \sqrt{3}\, V_r = (1 + \sqrt{3})\, (A_1 + \sqrt{3}\, B_1)^r.$$

The cases (a) - (o) in [22] can be tackled easily by using our relations (23) (with D = 3), (24), (39) - (42) and (6) - (9).

4. GENERALIZATION OF A THEOREM OF A. BRAUER

In [5], A.Brauer proved the following :

THEOREM 3.17. Let i and j be different positive integers and p be a prime. The system of simultaneous Diophantine equations

$$\left.\begin{aligned} x^2 + x + 1 &= 3p^i \\ y^2 + y + 1 &= 3p^j \end{aligned}\right\} \tag{66}$$

has no solutions in positive integers x,y.

In this section we generalize Brauer's result and prove the following :

THEOREM 3.18. Let i and j be different positive integers. The system of simultaneous Diophantine equations

$$\left.\begin{aligned} x^2 + x + 1 &= 3z^i \\ y^2 + y + 1 &= 3z^j \end{aligned}\right\} \tag{67}$$

has no integral solutions except z = 1.

Proof. In [20], T.Nagell proved that the Diophantine equation

$$x^2 + x + 1 = 3z^m \ (m > 2)$$

has no solution with $z > 1$. Hence we have only to consider the cases $i = 1$, $j = 2$; $i = 2$, $j = 1$. It is enough to consider $i = 1$, $j = 2$. i.e.,

$$x^2 + x + 1 = 3z \tag{68}$$

and

$$y^2 + y + 1 = 3z^2. \tag{69}$$

(68) and (69) imply $3 \mid x^2+x+1$ and $3 \mid y^2+y+1$. Thus $x \equiv y \equiv 1 \pmod 3$. From (68) and (69) we have $c^2 = 3\,(y^2+y+1)$ where $c = x^2+x+1$. Then

$$(2c)^2 - 3(2y+1)^2 = 9.$$

i.e.,

$$e^2 - 3f^2 = 9$$

where $e = 2c$, $f = 2y+1$. We have $e \equiv f \equiv 0 \pmod 3$. So we obtain

$$A^2 - 3B^2 = 1 \tag{70}$$

where $A = \frac{e}{3}$, $B = \frac{f}{3}$. Thus, in order to solve the system (68) and (69), we have to solve (70) with the restrictions $A = \frac{2(x^2+x+1)}{3}$. i.e., $6A - 3 = Z^2$ where $Z = 2x + 1$ and $B = \frac{2y+1}{3}$, an integer. The latter restriction is always satisfied since $y \equiv 1 \pmod 3$. So we have to check $2 \mid A$ and $6A-3 = Z^2$.

The fundamental solution of (70) is $a = A_1 = 2$, $b = B_1 = 1$. So the general solution of (70) is given by

$$A_r + \sqrt{3}\,B_r = (2+\sqrt{3})^r.$$

We need the following table of values :

r	A_r	B_r
0	1	0
1	2	1
2	7	4
3	26	15
4	97	56
5	362	209
6	1351	780
7	5042	2911
8	18817	10864
9	70226	40545
10	262087	151316
11	978122	564719
12	3650401	2107560

Table 2

We perform the calculations in five stages.

(a) From (16), we have $A_{r+2} \equiv A_r \pmod 2$. Since $A_o \equiv 1 \pmod 2$, it follows that $A_r \equiv 1 \pmod 2$ for all even values of r. But we want A such that $2|A$. Hence r cannot be even.

(b) From (2), we have $A_{r+3} = 26A_r + 45B_r$. This yields $A_{r+3} \equiv A_r \pmod{5}$. If $r \equiv 0 \pmod{3}$, then $A_r \equiv A_0 \pmod{5} \equiv 1 \pmod{5}$. So $z^2 = 6A_r - 3 \equiv 3 \pmod{5}$. But $\left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1$. Thus $r \not\equiv 0 \pmod{3}$.

(c) From (39)′, $A_{r+6} \equiv -A_r \pmod{A_3} \equiv -A_r \pmod{26}$. This implies $A_{r+12} \equiv A_r \pmod{13}$. If $r \equiv 5 \pmod{12}$, then $A_r \equiv A_5 \pmod{13} \equiv 11 \pmod{13}$. Hence $z^2 = 6A_r - 3 \equiv 11 \pmod{13}$. However, $\left(\frac{11}{13}\right) = \left(\frac{2}{11}\right) = -1$. So $r \not\equiv 5 \pmod{12}$. Next, if $r \equiv 7 \pmod{12}$, then $A_r \equiv A_7 \pmod{13} \equiv A_{-5} \pmod{13} \equiv A_5 \pmod{13}$, using (14). This again leads to a contradiction. Therefore $r \not\equiv 7 \pmod{12}$.

Now it remains to consider the cases $r \equiv 1, 11 \pmod{12}$.

(d) $z^2 = 6A_r - 3$ is impossible if $r \equiv 1 \pmod{12}$, $r \neq 1$.

For, we can write $r = 1 + 2k \cdot 3h$ where $k = 2^t$, $t \geq 1$ and h is an odd integer. Using (39)′ h times, we obtain

$$A_r \equiv -A_1 \pmod{A_{3k}}$$

$$\equiv -2 \pmod{A_k(4A_k^2 - 3)}.$$

Hence $z^2 \equiv -15 \pmod{A_k}$. Now,

$$\left(\frac{-15}{A_k}\right) = \left(\frac{-1}{A_k}\right)\left(\frac{3}{A_k}\right)\left(\frac{5}{A_k}\right).$$

Using (6), by induction we have $A_k \equiv 3 \pmod{4}$ for $t = 1$ and $1 \pmod{4}$ for $t \geq 2$; $1 \pmod{3}$ for $t \geq 1$ and $2 \pmod{5}$ for $t \geq 1$. Hence, for $t = 1$, we have

$$\left(\frac{-15}{A_k}\right) = -\left(\frac{3}{A_k}\right)\left(\frac{5}{A_k}\right) = \left(\frac{A_k}{3}\right)\left(\frac{A_k}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = -1,$$

and for $t \geq 2$, we have

$$\left(\frac{-15}{A_k}\right) = \left(\frac{3}{A_k}\right)\left(\frac{5}{A_k}\right) = \left(\frac{A_k}{3}\right)\left(\frac{A_k}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = -1.$$

Hence $z^2 = 6A_r - 3$ is impossible when $r \equiv 1 \pmod{12}$ with $r \neq 1$.

(e) $z^2 = 6A_r - 3$ is impossible if $r \equiv 11 \pmod{12}$, $r \neq 11$. A proof similar to that for (d) applies here and we make use of (14).

Combining (a), (b), (c), (d) and (e) we see that $z^2 = 6A_r - 3$ cannot hold for $r \neq 1, 11$. For $r = 1$, we have $A_r = 2$, $B_r = 1$, $x = 1, -2$, $y = 1$, $z = 1$ and for $r = 11$, we have $A_r = 978122$, $B_r = 564719$, $x^2 + x - 1467182 = 0$ from which we do not get integral x. This completes the proof of Theorem 3.18.

5. NUMBERS WITH PROPERTY P_k

For a history of our problem, we refer to L.E. Dickson [12]. Diophantus, III, 12, 13 and IV, 20 asked for three numbers such that the product of any two increased by a given number a shall be a square. For $a = 12$, he found $2, 2, \frac{1}{8}$; for $a = -10$, complicated fractions; for $a = 1, x, x+2,$

$4x+4$. In V, 27, the numbers themselves are to be squares. In IV, 21, he required four numbers such that the product of any two increased by unity is a square. He took x, $x+2$, $4x+4$ as the first three (by IV, 20) and $(3x+1)^2 - 1$ as the product of the first and fourth. Thus the fourth is $9x+6$. The product of the second and fourth, increased by unity, is $9x^2 + 24x + 13$; let it equal $(3x-4)^2$, whence $x = \frac{1}{16}$. The remaining conditions are now satisfied. Fermat took 1,3,8 as the first three numbers. The conditions on the fourth number x are $x+1 = \square$, $3x+1 = \square$, $8x+1 = \square$. His method of solving a "triple equation" gives $x = 120$.

M. Gardner [14] asked for a fifth number that can be added to the set $\{1,3,8,120\}$ without destroying the property that the product of any two integers is one less than a perfect square. In [18], J.H. van Lint proved that the system

$$\left.\begin{aligned} \rho + 1 &= x^2 \\ 3\rho + 1 &= y^2 \\ 8\rho + 1 &= z^2 \end{aligned}\right\} \qquad (70)'$$

has no solutions ρ with $120 < \rho < 10^{200}$. In [19] he proved that $(70)'$ has no solutions ρ with $120 < \rho < 10^{1700000}$, by performing the computation using a computer. A.Baker and

H. Davenport [4] proved that there exists no other positive integer ρ which can be included in the set $\{1,3,8,120\}$, by using the theory of Diophantine approximation. P. Kanagasabapathy and Tharmambikai Ponnudurai [17] gave another proof for the same result, using quadratic reciprocity. J. Arkin, V.E.Hoggatt, Jr. and E.G. Straus [1,2] and B.W. Jones [15,16] considered this problem from algebraic point of view.

Based on the work of the above-mentioned authors, we give the following

DEFINITION 3.4. Let k be a given positive integer. Two integers α and β are said to have the property p_k (resp. p_{-k}) if $\alpha\beta+k$ (resp. $\alpha\beta-k$) is a perfect square.

First we have a theorem for the Fibonacci sequence. The Fibonacci sequence $\{F_n\}$ is defined by

$$\left.\begin{aligned} F_1 &= F_2 = 1, \\ F_{n+2} &= F_{n+1} + F_n. \end{aligned}\right\} \quad (71)$$

THEOREM 3.19. F_{2j} and $F_{2(j+n)}$ have the property p_k while F_{2j+1} and $F_{2(j+n)}$ have the property p_{-k} where $k = F_n^2$.

In the following theorems we give some polynomials which produce 4 numbers sharing the property p_k for some k.

THEOREM 3.20. Let α be a given integer ≥ 2. Let d_1, d_2 be two positive divisors of α^2-1 such that $d_1 < d_2$. Then d_1, d_2, $d_1+d_2+2\alpha$, $4\alpha(d_1+\alpha)(d_2+\alpha)$ share the property p_1.

THEOREM 3.21. Let α be a given integer ≥ 3. Let d_1, d_2 be two positive divisors of α^2-4 such that $d_1 < d_2$. Then d_1, d_2, $d_1+d_2+2\alpha$, $\alpha(d_1+\alpha)(d_2+\alpha)$ share the property p_4.

THEOREM 3.22. Let α be any given non-zero integer. Then α^2-1, α^2, $4\alpha^2-1$, $16\alpha^4-8\alpha^2$ share the property p_{α^2}.

THEOREM 3.23. Let α be a given positive integer such that $4\alpha+1$ is a perfect square. Then $1, 4\alpha^2, 4\alpha^3+\alpha^2-4\alpha-1, 16\alpha^4+8\alpha^3-7\alpha^2-6\alpha$ share the property $p_{4\alpha+1}$.

THEOREM 3.24. If α is a non-zero integer, then $\alpha^2, 2\alpha^3+\alpha^2$, $4\alpha^3+4\alpha^2$, $12\alpha^3+44\alpha^2+48\alpha+16$ share the property p_{α^6}.

6. THE SIMULTANEOUS DIOPHANTINE EQUATIONS $10V^2+6 = U^2$ AND $26V^2+22 = Z^2$

The three numbers 2,5 and 13 share the property p_{-1}. We determine which other numbers can be in the set 2,5,13,... which will share the property p_{-1} with 2,5,13.

Let w be any other number in the set 2,5,13,.... Then

$$2w - 1 = x^2 \tag{72}$$

$$5w - 1 = y^2 \tag{73}$$

$$13w - 1 = z^2 \tag{74}$$

where x,y,z are some integers. Elimination of w between (72) and (73) and that between (72) and (74) yield

$$U^2 - 10V^2 = 6, \tag{75}$$

$$Z^2 - 26V^2 = 22 \tag{76}$$

respectively, where $U = 2y$, $V = x$, $Z = 2z$. So we have to obtain the solutions of the Pell's equation (75) with the restriction given by (76).

The Pell's equation

$$A^2 - 10B^2 = 1$$

has the fundamental solution $A_1 = 19$, $B_1 = 6$. The equation (75) has two non-associated classes of solutions and the fundamental solutions are $4 - \sqrt{10}$ and $4 + \sqrt{10}$ respectively. So the general solution of (75) is given by

$$U_r + \sqrt{10}\, V_r = (4 - \sqrt{10})\,(19 + 6\sqrt{10})^r, \qquad (77)$$

$$U_r + \sqrt{10}\, V_r = (4 + \sqrt{10})\,(19 + 6\sqrt{10})^r \qquad (78)$$

respectively.

First we consider (77). We need the following tables of values :

r	A_r	B_r
0	1	0
1	19	6
2	721	228
3	27379	8658
4	1039681	328776
5	39480499	12484830
6	1499219281	474094764

Table 3

r	U_r	V_r
0	4	-1
1	16	5
2	604	191
3	22936	7253
4	870964	275423
5	33073696	10458821
6	1255929484	397159775

Table 4

The calculations are performed in 3 stages.

(a) From (42), $V_{r+4} \equiv V_r \pmod{B_2} \equiv V_r \pmod{228} \equiv V_r \pmod{19}$. From (76), $Z^2 \equiv 7V_r^2 + 3 \pmod{19}$. If $r \equiv 0 \pmod 4$, then $V_r \equiv V_0 \pmod{19} \equiv 18 \pmod{19}$. This implies $Z^2 \equiv 10 \pmod{19}$. But $(\frac{10}{19}) = (\frac{2}{19})(\frac{5}{19}) = -(\frac{19}{5}) = -1$. So $r \not\equiv 0 \pmod 4$. If $r \equiv 2 \pmod 4$, then $V_r \equiv V_2 \pmod{19} \equiv 1 \pmod{19}$. This gives $Z^2 \equiv 10 \pmod{19}$, a contradiction again. Hence $r \not\equiv 2 \pmod 4$.

(b) From (24), $V_{r+3} = 8658U_r + 27379 V_r \equiv V_r \pmod 9$. (76) implies $Z^2 \equiv 8V_r^2 + 4 \pmod 9$. If $r \equiv 0 \pmod 3$, then $V_r \equiv V_1 \pmod 9 \equiv 8 \pmod 9$. Hence $Z^2 \equiv 3 \pmod 9$, which is impossible. So $r \not\equiv 0 \pmod 3$. If $r \equiv 1 \pmod 3$, then $V_r \equiv V_1 \pmod 9 \equiv 5 \pmod 9$. This gives $Z^2 \equiv 6 \pmod 9$, which is also impossible. Thus $r \not\equiv 1 \pmod 3$. Now the remaining case is $r \equiv 2 \pmod 6$.

(c) From (42), $V_{r+12} \equiv V_r \pmod{B_6} \equiv V_r \pmod{474094764} \equiv V_r \pmod{131}$. (76) implies $Z^2 \equiv 26V_r^2 + 22 \pmod{131}$. If $r \equiv 2$

(mod 12), then $V_r \equiv V_2 \pmod{131} \equiv 60 \pmod{131}$. So $z^2 \equiv 88$ (mod 131). But $\left(\frac{88}{131}\right) = \left(\frac{2}{131}\right)\left(\frac{11}{131}\right) = \left(\frac{10}{11}\right) = -\left(\frac{11}{5}\right) = -1$. Hence $r \not\equiv 2 \pmod{12}$. Next, if $r \equiv 8 \pmod{12}$, then $V_r \equiv V_8$ (mod 131) $\equiv -60 \pmod{131}$. This leads to a contradiction again. Hence $r \not\equiv 8 \pmod{12}$.

Combining (a), (b) and (c) we see that $z^2 = 26V_r^2 + 22$ cannot hold for any r.

Next we consider (78). In this case we have the following table of values :

r	U_r	V_r
0	4	1
1	136	43
2	5164	1633
3	196096	62011
4	7446484	2354785
5	282770296	89419819
6	10737824764	3395598377

Table 5

For (78) we can proceed exactly as we did for (77) and see that there is no integer r such that $U_r^2 - 10V_r^2 = 6$ and $z^2 - 26V_r^2 = 22$ hold simultaneously.

As we have exhausted all the possibilities, we have the

THEOREM 3.25. There is no other positive integer ρ which shares the property P_{-1} with 2,5 and 13.

7. THE SIMULTANEOUS DIOPHANTINE EQUATIONS $65V^2+40 = U^2$ AND $170V^2+145 = Z^2$

The three numbers 5, 13 and 34 share the property p_{-1}. We determine which other numbers can be in the set 5, 13, 34,... which will share the property p_{-1} with 5, 13, 34.

Let w be any other number in the set 5, 13, 34,.... Then

$$5w - 1 = x^2 \tag{79}$$

$$13w - 1 = y^2 \tag{80}$$

$$34w - 1 = z^2 \tag{81}$$

where x,y,z are some integers. Elimination of w between (79) and(80) and that between (79) and (81) yield

$$U^2 - 65V^2 = 40, \tag{82}$$

$$Z^2 - 170V^2 = 145 \tag{83}$$

respectively, where $U = 5y$, $V = x$, $Z = 5z$. So we have to obtain the solutions of the Pell's equation (82) with the restriction given by (83).

The Pell's equation

$$A^2 - 65B^2 = 1$$

has the fundamental solution $A_1 = 129$, $B_1 = 16$. The equation (82) has two non-associated classes of solutions and the fundamental solutions are $25 - 3\sqrt{65}$ and $25 + 3\sqrt{65}$ respectively. So the general solution of (82) is given by

$$U_r + \sqrt{65}\, V_r = (25-3\sqrt{65})\,(129+16\sqrt{65})^r, \tag{84}$$

$$U_r + \sqrt{65}\, V_r = (25+3\sqrt{65})\,(129+16\sqrt{65})^r \tag{85}$$

respectively.

First we consider (84). We need the following tables of values :

r	A_r	B_r
0	1	0
1	129	16
2	33281	4128
3	8586369	1065008
4	2215249921	274767936

Table 6

r	U_r	V_r
0	25	-3
1	105	13
2	27065	3357
3	6982665	866093
4	1801500505	223448637

Table 7

The calculations are performed in 3 stages.

(a) From (42), $V_{r+4} \equiv V_r \pmod{B_2} \equiv V_r \pmod{4128} \equiv V_r \pmod{43}$. (83) implies $Z^2 \equiv 41V_r^2 + 16 \pmod{43}$. If $r \equiv 1 \pmod 4$, then $V_r \equiv V_1 \pmod{43} \equiv 13 \pmod{43}$. This gives $Z^2 \equiv 22 \pmod{43}$.

But $(\frac{22}{43}) = -(\frac{11}{43}) = (\frac{-1}{11}) = -1$. Hence $r \not\equiv 1 \pmod 4$. Next, if $r \equiv 3 \pmod 4$, then $V_r \equiv V_3 \pmod{43} \equiv -13 \pmod{43}$ which also gives a contradiction. So $r \not\equiv 3 \pmod 4$. It remains to consider the even values for r.

(b) From (41), $V_{r+4} \equiv -V_r \pmod{A_2} \equiv -V_r \pmod{33281} \equiv -V_r \pmod{23}$. Hence $V_{r+8} \equiv V_r \pmod{23}$. From (83) we have $Z^2 \equiv 9V_r^2 + 7 \pmod{23}$. If $r \equiv 0 \pmod 8$, then $V_r \equiv V_0 \pmod{23} \equiv -3 \pmod{23}$. Hence $Z^2 \equiv 19 \pmod{23}$. But $(\frac{19}{23}) = (\frac{-1}{23}) = -1$. So $r \not\equiv 0 \pmod 8$. If $r \equiv 4 \pmod 8$, then $V_r \equiv V_4 \pmod{23} \equiv 3 \pmod{23}$, leading to a contradiction again. Thus $r \not\equiv 4 \pmod 8$.

(c) Again from (41), $V_{r+4} \equiv -V_r \pmod{33281} \equiv -V_r \pmod{1447}$. Therefore $V_{r+8} \equiv V_r \pmod{1447}$. From (83) we have $Z^2 \equiv 170V_r^2+145$. If $r \equiv 2 \pmod 8$, then $V_r \equiv V_2 \pmod{1447} \equiv 463 \pmod{1447}$. This gives $Z^2 \equiv 180 \pmod{1447}$. But $(\frac{180}{1447}) = (\frac{5}{1447}) = (\frac{2}{5}) = -1$. Hence $r \not\equiv 2 \pmod 8$. Next, if $r \equiv 6 \pmod 8$, then $V_r \equiv V_6 \pmod{1447} \equiv -463 \pmod{1447}$. This too gives a contradiction. So $r \not\equiv 6 \pmod 8$.

Combining (a), (b) and (c) we see that $Z^2=170V_r^2+145$ cannot hold for any r.

Next we consider (85). In this case we have the following table of values :

r	U_r	V_r
0	25	3
1	6345	787
2	1636985	203043
3	422335785	52384307

Table 8

For (85) we can proceed exactly as we did for (84) and see that there is no integer r such that $U_r^2 - 65V_r^2 = 40$ and $Z^2 - 170V_r^2 = 145$ hold simultaneously.

As we have exhausted all the possibilities, we have the

THEOREM 3.26. There is no other positive integer ρ which shares the property p_{-1} with 5, 13 and 34.

8. THE SIMULTANEOUS DIOPHANTINE EQUATIONS $2B^2+1 = A^2$ AND $5B^2-20 = Z^2$

The three numbers 1,5,10 share the property p_{-1}. We determine which other numbers can be in the set 1, 5, 10,... which will share the property p_{-1} with 1, 5, 10.

Let w be any other number in the set 1, 5, 10,... . Then

$$w - 1 = x^2 \tag{86}$$

$$5w - 1 = y^2 \tag{87}$$

$$10w - 1 = z^2 \tag{88}$$

where x,y,z are some integers. Elimination of w between (86) and (87) and that between (87) and (88) yield

$$Z^2 - 5B^2 = -20, \tag{89}$$

$$A^2 - 2B^2 = 1 \tag{90}$$

respectively, where $Z = 5x$, $B = y$, $A = z$. So we have to obtain the solutions of the Pell's equation (90) with the restriction given by (89).

The fundamental solution of (90) is $A_1 = 3$, $B_1 = 2$. We have the following table of values :

r	A_r	B_r
0	1	0
1	3	2
2	17	12
3	99	70
4	577	408
5	3363	2378
6	19601	13860
7	114243	80782
8	665857	470832
9	3880899	2744210
10	22619537	15994428

Table 9

We perform the calculations in five stages.

(a) From (42)′, $B_{r+8} \equiv B_r \pmod{B_4} \equiv B_r \pmod{408} \equiv B_r \pmod{17}$. (89) implies $Z^2 \equiv 5B_r^2 - 3 \pmod{17}$. If $r \equiv 0 \pmod 8$, then $B_r \equiv B_o \pmod{17} \equiv 0 \pmod{17}$. This gives $Z^2 \equiv -3 \pmod{17}$. But $(\frac{-3}{17}) = (\frac{-1}{17})(\frac{3}{17}) = (\frac{3}{17}) = (\frac{17}{3}) = (\frac{2}{3}) = -1$. So $r \not\equiv 0 \pmod 8$. Next, if $r \equiv 2 \pmod 8$, then $B_r \equiv B_2 \pmod{17} \equiv 12 \pmod{17}$. So $Z^2 \equiv 3 \pmod{17}$, which is impossible. Hence $r \not\equiv 2 \pmod 8$. If $r \equiv 4 \pmod 8$, then $B_r \equiv B_4 \pmod{17} \equiv 0 \pmod{17}$, which leads to a contradiction again. Thus $r \not\equiv 4 \pmod 8$. If $r \equiv 6 \pmod 8$,

then $r \equiv -2 \pmod 8$. So $B_r \equiv B_{-2} \pmod{17}$. Using (15), we get $B_r \equiv -B_2 \pmod{17} \equiv -12 \pmod{17}$, again yielding a contradiction. So $r \not\equiv 6 \pmod 8$. Hence we restrict ourselves to odd values of r in the sequel.

(b) Using (3), $B_{r+5} = 2378\ A_r + 3363\ B_r \equiv B_r \pmod{41}$. (89) implies $z^2 \equiv 5B_r^2 - 20 \pmod{41}$. If $r \equiv 2 \pmod 5$, then $B_r \equiv B_2 \pmod{41} \equiv 12 \pmod{41}$. Hence $z^2 \equiv 3 \pmod{41}$. But $(\frac{3}{41}) = (\frac{41}{3}) = (\frac{2}{3}) = -1$. So $r \not\equiv 2 \pmod 5$. If $r \equiv 3 \pmod 5$, then $B_r \equiv B_3 \pmod{41} \equiv -12 \pmod{41}$, again giving a contradiction. Therefore $r \not\equiv 3 \pmod 5$.

(c) Using (41)', $B_{r+20} \equiv -B_r \pmod{A_{10}} \equiv -B_r \pmod{22619537}$ $\equiv -B_r \pmod{241}$. This gives $B_{r+40} \equiv B_r \pmod{241}$. (89) implies $z^2 \equiv 5B_r^2 - 20 \pmod{241}$. If $r \equiv \pm 5 \pmod{40}$, then $B_r \equiv \mp 32 \pmod{241}$. Hence $z^2 \equiv 39 \pmod{241}$. But $(\frac{39}{241}) = (\frac{3}{241})(\frac{13}{241}) = (\frac{1}{3})(\frac{7}{13}) = (\frac{6}{7}) = -1$. So $r \not\equiv \pm 5 \pmod{40}$. Next, if $r \equiv \pm 9 \pmod{40}$, then $B_r \equiv \mp 57 \pmod{241}$. This gives $z^2 \equiv 78 \pmod{241}$. However, $(\frac{78}{241}) = (\frac{2}{241})(\frac{3}{241})(\frac{13}{241}) = -1$. This forces $r \not\equiv \pm 9 \pmod{40}$. If $r \equiv \pm 11 \pmod{40}$, then $B_r \equiv \mp 57 \pmod{241}$, leading to a contradiction again. So $r \not\equiv \pm 11 \pmod{40}$. If $r \equiv \pm 15 \pmod{40}$, then $B_r \equiv \mp 32 \pmod{241}$, again a contradiction. Hence $r \not\equiv \pm 15 \pmod{40}$. Consequently it remains to consider $r \equiv 1, 19, 21, 39 \pmod{40}$. i.e., $r \equiv \pm 1 \pmod{20}$.

(d) Next we prove that $z^2 = 5B_r^2 - 20$ is impossible if $r \equiv 1 \pmod{20}$, $r \neq 1$. The characteristic number of the system (90)

and (89), for $i = 1$, given by Definition 3.3, is 85. We have to find the values of t for which at least one of the $\left(\frac{85}{a_t^2+2b_t^2}\right)$, $\left(\frac{85}{64b_{t+1}^4+24b_{t+1}^2+1}\right)$ is -1. Now $\left(\frac{85}{a_t^2+2b_t^2}\right) = \left(\frac{85}{a_{t+1}}\right) = \left(\frac{5}{a_{t+1}}\right)\left(\frac{17}{a_{t+1}}\right)$.

Using (6), by induction we have $a_{t+1} \equiv 1 \pmod 4$ for all $t \geq 1$; $2 \pmod 5$ for all $t \geq 1$; $-1 \pmod{17}$ for $t = 2$ and $1 \pmod{17}$ for all $t \geq 3$. Hence, for $t = 2$, we have

$$\left(\frac{5}{a_{t+1}}\right)\left(\frac{17}{a_{t+1}}\right) = \left(\frac{a_{t+1}}{5}\right)\left(\frac{a_{t+1}}{17}\right) = \left(\frac{2}{5}\right)\left(\frac{-1}{17}\right) = -1,$$

and for $t \geq 3$, we obtain

$$\left(\frac{5}{a_{t+1}}\right)\left(\frac{17}{a_{t+1}}\right) = \left(\frac{a_{t+1}}{5}\right)\left(\frac{a_{t+1}}{17}\right) = \left(\frac{2}{5}\right)\left(\frac{1}{17}\right) = -1.$$

Hence $\left(\frac{85}{a_t^2+2b_t^2}\right) = -1$ for all $t \geq 2$. This implies $Z^2 = 5B_r^2 - 20$ is impossible if $r \equiv 1 \pmod{20}$, $r \neq 1$.

(e) $Z^2 = 5B_r^2 - 20$ is impossible when $r \equiv 19 \pmod{20}$, $r \neq 19$. A proof similar to that for (d) applies here and we make use of (15).

Combining (a), (b), (c), (d) and (e) we see that $Z^2 = 5B_r^2 - 20$ cannot hold for $r \neq 1, 19$. For $r = 1$, we have $B_r = 2$, $w = 1$. For $r = 19$, we have $B_r \equiv 542 \pmod{1000}$. Hence $Z^2 = 5B_r^2 - 20 \equiv 800 \pmod{1000}$, which is impossible.

As we have exhausted all the possibilities, we have the

THEOREM 3.27. There is no other positive integer ρ which shares the property p_{-1} with 1, 5 and 10.

9. THE SIMULTANEOUS DIOPHANTINE EQUATIONS $5V^2-4 = U^2$ AND $12V^2-11 = Z^2$

The three numbers 1, 5, 12 share the property p_4. Let w be any other number in the set 1, 5, 12,..., sharing the property p_4. Then

$$w + 4 = x^2 \tag{91}$$

$$5w + 4 = y^2 \tag{92}$$

$$12w + 4 = z^2 \tag{93}$$

where x,y,z are some integers. Elimination of w between (91) and (92) and that between (91) and (93) yield

$$y^2 - 5x^2 = -16, \tag{94}$$

$$z^2 - 12x^2 = -44. \tag{95}$$

(94) implies $x \equiv y \pmod 2$. If y is odd, then $y^2 \equiv 1$ or 9 (mod 16). Hence $5x^2 \equiv 1$ or 9 (mod 16), which is impossible. Consequently x and y are both even. (93) implies z is even. Putting $x = 2V$, $y = 2U$, $z = 2Z$, the equations (94) and (95) are transformed as

$$U^2 - 5V^2 = -4, \tag{96}$$

$$Z^2 - 12V^2 = -11 \tag{97}$$

respectively. So we have to obtain the solutions of the Pell's equation (96) with the restriction given by (97).

The Pell's equation

$$A^2 - 5B^2 = 1$$

has the fundamental solution $A_1 = 9$, $B_1 = 4$. The equation (96) has three non-associated classes of solutions and the fundamental solutions are $-4 + 2\sqrt{5}$, $-1 + \sqrt{5}$ and $1 + \sqrt{5}$ respectively. So the general solution of (96) is given by

$$U_r + \sqrt{5}\, V_r = (-4 + 2\sqrt{5})\,(9 + 4\sqrt{5})^r, \tag{98}$$

$$U_r + \sqrt{5}\, V_r = (-1 + \sqrt{5})\,(9 + 4\sqrt{5})^r, \tag{99}$$

$$U_r + \sqrt{5}\, V_r = (1 + \sqrt{5})\,(9 + 4\sqrt{5})^r \tag{100}$$

respectively.

First we consider (98). We have the following tables of values :

r	A_r	B_r
0	1	0
1	9	4
2	161	72
3	2889	1292
4	51841	23184
5	930249	416020
6	16692641	7465176
7	299537289	133957148
8	5374978561	2403763488

Table 10

r	U_r	V_r
0	-4	2
1	4	2
2	76	34
3	1364	610
4	24476	10946
5	439204	196418
6	7881196	3524578
7	141422324	63245986
8	2537720636	1134903170

Table 11

From (24), we have $V_{r+3} = 1292U_r + 2889V_r \equiv V_r \pmod{19}$. (97) implies $Z^2 \equiv 12V_r^2 - 11 \pmod{19}$. If $r \equiv 0 \pmod 3$, then $V_r \equiv V_0 \pmod{19} \equiv 2 \pmod{19}$. This implies $Z^2 \equiv 18 \pmod{19}$. But $(\frac{18}{19}) = (\frac{2}{19}) = -1$. So $r \not\equiv 0 \pmod 3$. If $r \equiv 1 \pmod 3$, then $V_r \equiv V_1 \pmod{19} \equiv 2 \pmod{19}$, again leading to a contradiction. If $r \equiv 2 \pmod 3$, then $V_r \equiv V_2 \pmod{19} \equiv 15 \pmod{19}$. Hence $Z^2 \equiv 10 \pmod{19}$. However, $(\frac{10}{19}) = (\frac{2}{19})(\frac{5}{19}) = -(\frac{19}{5}) = -(\frac{-1}{5}) = -1$. Therefore there exists no integer r such that V_r simultaneously satisfies (96) and (97). Consequently there results no integral value for w from (98).

Next we consider (99). In this case we have the following table of values :

r	U_r	V_r
0	-1	1
1	11	5
2	199	89
3	3571	1597
4	64079	28657
5	1149851	514229
6	20633239	9227465
7	370248451	165580141
8	6643838879	2971215073
9	119218851371	53316291173
10	2139295485799	956722026041

Table 12

We perform the calculations in 4 stages.

(a) From (24), $V_{r+5} = 416020U_r + 930249V_r \equiv V_r \pmod{31}$. (97) implies $Z^2 \equiv 12V_r^2 - 11 \pmod{31}$. If $r \equiv 2 \pmod 5$, then $V_r \equiv V_2 \pmod{31} \equiv 27 \pmod{31}$. This gives $Z^2 \equiv 26 \pmod{31}$. However, $(\frac{26}{31}) = (\frac{2}{31})(\frac{13}{31}) = (\frac{31}{13}) = (\frac{13}{5}) = (\frac{5}{3}) = (\frac{2}{3}) = -1$. Hence $r \not\equiv 2 \pmod 5$. Next, if $r \equiv 3 \pmod 5$, then $V_r \equiv V_3 \pmod{31} \equiv 16 \pmod{31}$. So $Z^2 \equiv 23 \pmod{31}$. But $(\frac{23}{31}) = (\frac{-1}{31})(\frac{2}{31}) = -1$. Thus $r \not\equiv 3 \pmod 5$.

(b) From (42), $V_{r+10} \equiv V_r \pmod{B_5} \equiv V_r \pmod{416020} \equiv V_r \pmod 5$. (97) implies $Z^2 \equiv 2V_r^2 - 1 \pmod 5$. If $r \equiv 4 \pmod{10}$, then $V_r \equiv V_4 \pmod 5 \equiv 2 \pmod 5$. Hence $Z^2 \equiv 2 \pmod 5$. But

$(\frac{2}{5}) = -1$. So $r \not\equiv 4 \pmod{10}$. Next, if $r \equiv 9 \pmod{10}$, then $V_r \equiv V_9 \pmod 5 \equiv -2 \pmod 5$. This leads to a contradiction again. Hence $r \not\equiv 9 \pmod{10}$.

(c) From (41), $V_{r+10} \equiv -V_r \pmod{A_5} \equiv -V_r \pmod{930249} \equiv -V_r \pmod{41}$. This implies $V_{r+20} \equiv V_r \pmod{41}$. From (97), we have $Z^2 \equiv 12V_r^2 - 11 \pmod{41}$. If $r \equiv 5 \pmod{20}$, then $V_r \equiv V_5 \pmod{41} \equiv 7 \pmod{41}$. Hence $Z^2 \equiv 3 \pmod{41}$. But $(\frac{3}{41}) = (\frac{2}{3}) = -1$. Therefore $r \not\equiv 5 \pmod{20}$. Next, if $r \equiv 15 \pmod{20}$, then $V_r \equiv -7 \pmod{41}$. This also gives a contradiction. So $r \not\equiv 15 \pmod{20}$.

(d) Next we prove that $Z^2 = 12V_r^2 - 11$ is impossible if $r \equiv 0 \pmod{10}$, $r \neq 0$. The characteristic number of the system (96) and (97) for $i = 0$, given by Definition 3.3, is 67. We have to find the values of t for which at least one of $(\frac{67}{a_t^2+5b_t^2})$, $(\frac{67}{400b_{t+1}^4+60b_{t+1}^2+1})$ is -1. Now $(\frac{67}{a_t^2+5b_t^2}) = (\frac{67}{a_{t+1}})$. Using (6), by induction we obtain $a_{t+1} \equiv 1 \pmod 4$ for all $t \geq 1$. For $t = 1$ we have $a_{t+1} \equiv 27 \pmod{67}$ and when $t \geq 2$, we have $a_{t+1} \equiv 11, 40, 50, 41 \pmod{67}$ respectively for $t \equiv 0,1,2,3 \pmod 4$. Since $(\frac{67}{a_{t+1}}) = (\frac{a_{t+1}}{67})$ and $(\frac{27}{67})$, $(\frac{11}{67})$, $(\frac{50}{67})$ and $(\frac{41}{67})$ all equal -1, we see that $Z^2 = 12V_r^2 - 11$ is impossible if $t = 1$ or if $t \equiv 0,2,3 \pmod 4$ and $t \geq 2$. Using (6) and (7), by induction we get $b_{t+1} \equiv 5 \pmod{67}$ for $t = 1$ and $b_{t+1} \equiv 15, 62, 2, 66, 52, 5, 65, 1 \pmod{67}$ for $t \equiv 0,1,2,3,4,5,6,7 \pmod 8$ respectively when $t \geq 2$. If $t \equiv 1$ or $5 \pmod 8$ and $t \geq 2$, then we have

$$\left(\frac{67}{400b_{t+1}^4+60b_{t+1}^2+1}\right) = \left(\frac{400b_{t+1}^4+60b_{t+1}^2+1}{67}\right)$$

$$= \left(\frac{65b_{t+1}^4+60b_{t+1}^2+1}{67}\right) = \left(\frac{50}{67}\right) = \left(\frac{2}{67}\right) = -1.$$

Hence $Z^2 = 12V_r^2 - 11$ is impossible if $t \equiv 1 \pmod 4$ and $t \geq 2$. Consequently $Z^2 = 12V_r^2 - 11$ is impossible if $r \equiv 0 \pmod{10}$ and $r \neq 0$.

For $r = 0$, we have $U_r = -1$, $V_r = 1$ and $w = 0$.

Now it remains to consider $r \equiv 1,6 \pmod{10}$. From (42), we have $V_{r+10} \equiv V_r \pmod{10}$ for all r. If $r \equiv 1 \pmod{10}$, then $V_r \equiv V_1 \pmod{10} \equiv 5 \pmod{10}$ and so $w = 4(V_r^2 - 1) \equiv 96 \pmod{100}$. If $r \equiv 6 \pmod{10}$, then $V_r \equiv V_6 \pmod{10} \equiv 5 \pmod{10}$ and so $w \equiv 96 \pmod{100}$. Consequently if w is a positive integer which shares the property p_4 with 1, 5 and 12, then $w \equiv 96 \pmod{100}$.

For $r = 1$, we have $U_r = 11$, $V_r = 5$ and $w = 96$. We see that $w = 96$ shares the property p_4 with 1, 5 and 12. Now suppose there is a positive integer w', different from 96, which belongs to the set $\{1,5,12,96,\ldots\}$, sharing the property p_4. Then $w = 96$ and w' satisfy

$$ww' + 4 = L^2$$

for some integer L. Since $w' \equiv 96 \pmod{100}$, we have $L^2 \equiv 20$ mod 100), which is impossible. Hence (99) does not contribute ny positive integer ρ which shares the property p_4 with ,5,12 and 96.

Next we consider (100). In this case we have the following table of values :

r	U_r	V_r
0	1	1
1	29	13
2	521	233
3	9349	4181
4	167761	75025
5	3010349	1346269
6	54018521	24157817
7	969323029	433494437
8	17393796001	7778742049
9	312119004989	139583862445
10	5600748293801	2504730781961

Table 13

For (100), we can proceed exactly as we did for (99) and check that there does not result any positive integer ρ sharing the property p_4 with 1, 5, 12 and 96. Thus we have established the

THEOREM 3.28. There is no other positive integer ρ which shares the property p_4 with 1, 5, 12 and 96.

10. THE SIMULTANEOUS DIOPHANTINE EQUATIONS $2x^2-1 = y^2$ AND $6x^2-5 = z^2$

The three numbers 2, 4, 12 share the property p_1. Let w be any other number in the set 2, 4, 12,..., sharing the property

p_1. Then

$$2w + 1 = x^2 \tag{101}$$

$$4w + 1 = y^2 \tag{102}$$

$$12w + 1 = z^2 \tag{103}$$

where x, y, z are some integers. Elimination of w between (101) and (102) and that between (101) and (103) yield

$$y^2 - 2x^2 = -1 \tag{104}$$

$$z^2 - 6x^2 = -5 \tag{105}$$

respectively. So we have to obtain the solutions of the Pell's equation (104) with the restriction given by (105).

We follow the method of A. Baker and H. Davenport [4]. The fundamental solution of (104) is $y=1$, $x=1$. So the general solution of (104) is given by

$$y + x\sqrt{2} = (1+\sqrt{2})\ (3+2\sqrt{2})^m \tag{106}$$

where m is an integer. Hence

$$y - x\sqrt{2} = (1-\sqrt{2})\ (3-2\sqrt{2})^m.$$

Consequently

$$2\sqrt{2}\ x = (1+\sqrt{2})\ (3+2\sqrt{2})^m - (1-\sqrt{2})(3-2\sqrt{2})^m. \tag{107}$$

For $m=0$, we have $x=1$, $y=1$, $w=0$ and for $m=2$, we have $x = 29$, $y = 41$, $w = 420$. The equation (105) has two non-associated classes of solutions and the fundamental solutions are $1+\sqrt{6}$ and $-1+\sqrt{6}$ respectively. So the general solution of (105) is given by

$$z + \sqrt{6}\ x = (1+\sqrt{6})\ (5+2\sqrt{6})^n, \tag{108}$$

$$z + \sqrt{6}\ x = (-1+\sqrt{6})(5+2\sqrt{6})^n \tag{109}$$

respectively, where n is an integer. From (108) and (109), we get

$$2\sqrt{6}\,x = (1+\sqrt{6})(5+2\sqrt{6})^n - (1-\sqrt{6})(5-2\sqrt{6})^n \tag{110}$$

$$2\sqrt{6}\,x = (-1+\sqrt{6})(5+2\sqrt{6})^n - (-1-\sqrt{6})(5-2\sqrt{6})^n \tag{111}$$

respectively. For $n=0$, we have $x=1$, $z=1$, $w=0$ in (108) and $x=1$, $z=-1$, $w=0$ in (109). For $n=2$, we have $x=29$, $z=71$, $w=420$ in (109) and for $n=-2$, we have $x=29$, $z=-71$, $w=420$ in (108).

We seek the common values of (107) and either (110) or (111). We consider first (107) and (110). Here

$$\begin{aligned} 2x &= \frac{1+\sqrt{2}}{\sqrt{2}}(3+2\sqrt{2})^m + \frac{\sqrt{2}-1}{\sqrt{2}}(3+2\sqrt{2})^{-m} \\ &= \frac{1+\sqrt{6}}{\sqrt{6}}(5+2\sqrt{6})^m + \frac{\sqrt{6}-1}{\sqrt{6}}(5+2\sqrt{6})^{-n}. \end{aligned}$$ Let us put

$$\left.\begin{aligned} P &= \frac{1+\sqrt{2}}{\sqrt{2}}(3+2\sqrt{2})^m, \\ Q &= \frac{1+\sqrt{6}}{\sqrt{6}}(5+2\sqrt{6})^n. \end{aligned}\right\} \tag{112}$$

Then we must have

$$P + \frac{1}{2}P^{-1} = Q + \frac{5}{6}Q^{-1}$$

for some integers m and n. We consider $m, n \geq 0$ and fix m and n. Since

$$\begin{aligned} P-Q &= \frac{5}{6}Q^{-1} - \frac{1}{2}P^{-1} > \frac{1}{2}Q^{-1} - \frac{1}{2}P^{-1} \\ &= \frac{1}{2}(P-Q)P^{-1}Q^{-1}, \end{aligned}$$

and $P>1$, $Q>1$, we must have $Q<P$. Let us suppose that $m\geq 3$. Then

and

$$Q > P - \frac{5}{6} Q^{-1} > P - \frac{5}{6} .$$

Hence

$$P-Q = \frac{5}{6} Q^{-1} - \frac{1}{2} P^{-1} < \frac{5}{6} (P- \frac{5}{6})^{-1} - \frac{1}{2} P^{-1} < \frac{17}{50} P^{-1} .$$

It follows that

$$0 < \log(\frac{P}{Q}) = -\log (1- \frac{P-Q}{P}) < \frac{17}{50} P^{-2} + (\frac{17}{50} P^{-2})^2$$
$$< 0.4556 P^{-2} .$$

Substituting from (112) we get

$$0 < m \log (3+2\sqrt{2}) - n \log (5+2\sqrt{6}) + \log \frac{(1+\sqrt{2})\sqrt{6}}{(1+\sqrt{6})\sqrt{2}}$$
$$< 0.4556 P^{-2} < \frac{0.16}{(3+2\sqrt{2})^{2m}} . \tag{113}$$

DEFINITION 3.5. The height of an algebraic number is the maximum of the absolute values of the relatively prime integer coefficients in its minimal defining polynomial.

THEOREM 3.29. (A. Baker [3]). Suppose that $k \geq 2$ and that $\alpha_1, \ldots, \alpha_k$ are non-zero algebraic numbers whose degrees do not exceed d and whose heights do not exceed A, where $d \geq 4$ and $A \geq 4$. If the rational integers $b_1, \ldots, b_k$ satisfy

$$0 < |b_1 \log \alpha_1 + \ldots + b_k \log \alpha_k| < e^{-\delta H} ,$$

where $0 < \delta \leq 1$ and

$$H = \max (|b_1|, \ldots, |b_k|),$$

then

$$H < (4^{k^2} \delta^{-1} d^{2k} \log A)^{(2k+1)^2} .$$

In this theorem the logarithms are supposed to have their principal values, but this is of no importance to us here, because we are concerned exclusively with positive algebraic numbers.

To apply Theorem 3.29 to our present problem, we take $k=3$, $\alpha_1 = 3+2\sqrt{2}$, $\alpha_2 = 5+2\sqrt{6}$, and $\alpha_3 = \dfrac{(1+\sqrt{2})\sqrt{6}}{(1+\sqrt{6})\sqrt{2}} = \dfrac{\sqrt{3}+\sqrt{6}}{\sqrt{6}+1}$.

The equations satisfied by α_1 and α_2 are

$$\alpha_1^2 - 6\alpha_1 + 1 = 0$$

and

$$\alpha_2^2 - 10\alpha_2 + 1 = 0,$$

respectively. Now we find the equation satisfied by α_3.

We have

$$\alpha_3 = \frac{\sqrt{3}+\sqrt{6}}{\sqrt{6}+1} = 1 - \frac{(1-\sqrt{3})}{\sqrt{6}+1}.$$

Hence

$$\alpha_3 - 1 = \frac{-(1-\sqrt{3})}{1+\sqrt{6}} = \frac{1+3\sqrt{2} - \sqrt{6} - \sqrt{3}}{5},$$

or, $5\alpha_3 - 6 = 3\sqrt{2} - \sqrt{6} - \sqrt{3}$. From this relation we obtain

$$25\alpha_3^2 - 60\alpha_3 + 9 = 6(\sqrt{2} - 2\sqrt{3} - \sqrt{6}).$$

Hence $(25\alpha_3^2 - 60\alpha_3 + 9)^2 = 36\ (20 + 4(3\sqrt{2} - \sqrt{6} - \sqrt{3}))$

$= 36(20 + 4(5\alpha_3 - 6)) = 720\ \alpha_3 - 144.$

i.e.,

$$25\alpha_3^4 - 120\alpha_3^3 + 162\alpha_3^2 - 72\alpha_3 + 9 = 0.$$

Hence $d=4$ and the maximum height of $\alpha_1, \alpha_2, \alpha_3$ is $A = 162$.

Since $0 < \log\left(\frac{P}{Q}\right) < \dfrac{0.16}{(3+2\sqrt{2})^{2m}}$ and $(3+2\sqrt{2})^2 > e$, we can tak

$\delta=1$. Since $n < m$, we can take $H=m$. Then by Theorem 3.29, we have

$$m < (4^9 \times 4^6 \times \log 162)^{49} < (4^{15} \times 5)^{49} < 10^{490}. \qquad (114)$$

If, in the foregoing argument, (110) is replaced by (111), the only difference is that α_3 is replaced by

$$\alpha'_3 = \frac{\sqrt{3} + \sqrt{6}}{\sqrt{6} - 1} .$$

Since α_3 and α'_3 satisfy the same equation, the conclusion (114) remains valid when (107) and (111) are considered.

It remains to consider the range

$$2 < m < 10^{490}. \qquad (115)$$

We have from (113)

$$0 < m \log \alpha_1 - n \log \alpha_2 + \log \alpha_3 < \frac{0.16}{(3+2\sqrt{2})^{2m}} .$$

This implies

$$0 < m \frac{\log \alpha_1}{\log \alpha_2} - n + \frac{\log \alpha_3}{\log \alpha_2} < \frac{0.16}{(3+2\sqrt{2})^{2m} \log \alpha_2} .$$

Putting

$$\theta = \frac{\log \alpha_1}{\log \alpha_2} , \qquad (116)$$

$$\beta = \frac{\log \alpha_3}{\log \alpha_2} \qquad (117)$$

we have

$$0 < m\theta - n + \beta < \frac{0.16}{(3+2\sqrt{2})^{2m} \log \alpha_2} .$$

Hence

$$|m\theta - n + \beta| < 0.0698 \; C^{-m} \qquad (118)$$

where $C = (3+2\sqrt{2})^2 = 33.968\ldots$.

In the alternative case, when (110) is replaced by (111), we have to replace β by

$$\beta' = \frac{\log \alpha_3'}{\log \alpha_2} . \tag{119}$$

i.e.,

$$\beta = \frac{\log(\frac{(1+\sqrt{2})\sqrt{3}}{\sqrt{6}+1})}{\log(5+2\sqrt{6})} \quad \text{and} \quad \beta = \frac{\log(\frac{(1+\sqrt{2})\sqrt{3}}{\sqrt{6}-1})}{\log(5+2\sqrt{6})} .$$

Let $||z||$ denote the distance of a real number z from the nearest integer.

LEMMA 3.30. (A. Baker and H. Davenport [4]) Suppose $K > 6$. For any positive integer M, let p and q be integers satisfying

$$\left.\begin{aligned} &1 \le q \le KM \text{ and} \\ &|\theta q - p| < 2(KM)^{-1} \end{aligned}\right\} \tag{120}$$

Then, if

$$||q\beta|| \ge 3K^{-1} , \tag{121}$$

there is no solution of (118) in the range

$$\frac{\log K^2 M}{\log C} < m < M. \tag{122}$$

To apply the Lemma 3.30 in our present problem, we take

$$M = 10^{490} \quad \text{and} \quad K = 10^{33}.$$

Let θ_0 be the value of θ correct to 1046 decimal places, so that

$$|\theta - \theta_0| < 10^{-1046} .$$

Let $\frac{p}{q}$ be the last convergent to the continued fraction for θ_0 whic

satisfies $q \leq 10^{523}$. Then

$$|q\theta_o - p| < 10^{-523} .$$

Hence

$$|q\theta - p| \leq q|\theta-\theta_o| + |q\theta_o - p| < 10^{-523} + 10^{-523}$$
$$= 2(KM)^{-1} .$$

Therefore the inequalities (120) are satisfied.

It follows from Lemma 3.30 that provided

$$\left.\begin{array}{l} ||q\beta|| \geq 3 \times 10^{-33} \quad \text{and} \\ ||q\beta'|| \geq 3 \times 10^{-33} \end{array}\right\} \qquad (121)'$$

there is no solution of (118), in either of the alternative forms, in the range

$$\frac{\log 10^{556}}{\log C} < m < 10^{490}$$

i.e.,

$$363 < m < 10^{490}.$$

To establish (121) for the problem of A. Baker and H. Davenport [4], they had to compute the four values θ, q, β, β' accurately to 1040, 520, 600, 600 decimal places, respectively. Thus Lemma 3.30 left them with this serious computational problem. They obtained the cooperation of the Atlas Computer Laboratory of the Science Research Council at Chilton, Berkshire, England. Mr. S.T.E. Muir, of that Laboratory, used a package originally developed by Mr. W.F. Lunnon, of Manchester University, to carry out multi-length arithmetic to an arbitrary precision.

By a remark of Baker and Davenport [4] it follows that if (121) were not satisfied, then although it could no longer be concluded that there is no value of m in the range

$$363 < m < 10^{490},$$

we can say that there is at most one value to the modulus q.

Now we consider the range

$$2 < m < 364.$$

We cclculate θ occurately to a few decimal places. We have

$$\theta = 0.7689420304.....$$

The first few convergents for the continued fraction for θ are

$$\frac{0}{1}, \frac{1}{1}, \frac{3}{4}, \frac{10}{13}, \frac{203}{264}, \frac{1025}{1333}, \frac{3278}{4263}, \frac{4303}{5596}.$$

We have

$$5596\,\theta - 4303 = -\,0.000\,118\,082\ldots$$

The inequality (118), after multiplication by 5596, gives

$$|m(4303+\Phi) - 5596n + 5596\beta| < 0.0698 \times 5596 \times (33.968)^{-m} \tag{123}$$

where $|\Phi| < 0.000119$. We have

$$|m\Phi| < 364 \times 0.000119 = 0.043316.$$

Since

$$\beta = 0.083951646\ldots,$$

$$\beta' = 0.4621590860\ldots$$

we find that

$$5596\beta \equiv 0.79341\ldots \pmod 1,$$

$$5596\beta' \equiv 0.242245\ldots \pmod 1.$$

Therefore (123) implies that

$$5596 \times 0.0698 \times (33.9)^{-m} > 0.242245 - 0.043316 > 0.19.$$

This gives a contradiction to the supposition that $m \geq 3$. Hence there is no common solution for (104) and (105) when $2 < m < 364$.

Summarizing the results, we see that (104) and (105) have no common solution when m satisfies $2 < m < 364$ or $m \geq 10^{490}$. For m satisfying $363 < m < 10^{490}$, at most one value of m to the modulus q may give a common solution for (104) and (105).

REFERENCES

1. J. Arkin, V.E. Hoggatt, Jr. and E.G. Straus, On Euler's solution of a problem of Diophantus, Fibonacci Quart., 17 (1979), 333-339. Zbl. 418. 10021.

2. ______, On Euler's solution of a problem of Diophantus-II, Fibonacci Quart., 18 (1980), 170-176. Zbl. 431. 10009.

3. A. Baker, Linear forms in the logarithms of algebraic numbers (IV), Mathematika, 15 (1968), 204-216. MR 41 # 3402.

4. ______ and H. Davenport, The equations $3x^2-2=y^2$ and $8x^2-7 = z^2$, Quart. J. Math. Oxford (2), 20(1969), 129-137. MR 40 # 1333.

5. A. Brauer, On the non-existence of odd perfect numbers of form $p^{\alpha} q_1^2 q_2^2 \cdots q_{t-1}^2 q_t^4$, Bull. Amer. Math. Soc., 49(1943), 712-718. MR 5, 90.

6. J.H.E. Cohn, Lucas and Fibonacci numbers and some Diophantine equations, Proc. Glasgow Math. Assoc., 7(1965), 24-28. MR 31 # 2202.

7. __________, Eight Diophantine equations, Proc. London Math. Soc. (3), 16(1966), 153-166. MR 32 # 7492. Addendum, ibid (3) 17 (1967), 381. MR 34 # 5748.

8. __________, Five Diophantine equations, Math. Scand., 21(1967), 61-70. MR 38 # 4401.

9. __________, Some quartic Diophantine equations, Pacific J. Math., 26 (1968), 233-243. MR 39 # 2702.

10. __________, The Diophantine equation $Y(Y+1)(Y+2)(Y+3) = 2X(X+1)(X+2)(X+3)$, Pacific J. Math., 37(1971), 331-335. MR 46 # 8969.

11. G.N. Copley, Recurrence relations for solutions of Pell's equation, Amer. Math. Monthly, 66(1959), 288-290. MR 21 #1951.

12. L.E. Dickson, History of the Theory of Number, Vol. II, Carnegie Institution, Washington, D.C., 1920.

13. E.I. Emerson, Recurrent sequences in the equation $DQ^2=R^2+N$, Fibonacci Quart., 7(1969), 231-242. MR 41 # 1628.

14. M. Gardner, Mathematical games, Scientific American, 216, No. 3 (1967), 124 and No. 4 (1967), 119.

15. B.W. Jones, A variation on a problem of Davenport and Diophantus, Quart. J. Math. Oxford (2), 27 (1976), 349-353. MR 58 # 575.

16. __________, A second variation on a problem of Diophantus and Davenport, Fibonacci Quart., 16 (1978), 155-165. MR 81h:10075.

17. P. Kanagasabapathy and Tharmambikai Ponnudurai, The simultaneous Diophantine equations $y^2-3x^2 = -2$ and $z^2-8x^2 = -7$, Quart. J. Math. Oxford (2), 26 (1975), 275-278. MR 52 # 8027.

18. J.H. Van Lint, Notitie 20 (1967), Technische Hogeschool Eindhoven.

19. ______________, On a set of Diophantine equations, T.H.-Report 68-WSK-03, The Dept. of Math., Technological University, Eindhoven, The Netherlands, 1968, 8pp. Zbl. 174, 79.

20. T. Nagell, Des equations indeterminees $x^2+x+1 = y^n$ et $x^2+x+1 = 3y^n$, Norske Matematisk Forenings, Skrifter (1), No. 2 (1921).

21. __________, Introduction to Number Theory, Wiley, New York, 1951. MR 13, 207.

22. Tharmambikai Ponnudurai, The Diophantine equation $Y(Y+1)(Y+2)(Y+3) = 3X(X+1)(X+2)(X+3)$, J. London Math. Soc. (2), 10 (1975), 232-240. MR 51 # 8025.

23. Manoranjitham Veluppillai, The Diophantine equation $(X[X-1])^2 = 3Y[Y-1]$, Glasgow Math. J., 17 (1976), 130-133. MR 54 # 13109.

CHAPTER 4

$P_{r,k}$ SEQUENCES

1. INTRODUCTION

In Chapter 3 (page 123), we have defined the notion of the property p_k (resp. p_{-k}) where k is a given positive integer. In this chapter we define a P_k set and a $P_{r,k}$ sequence. We provide a construction for a $P_{3,k}$ sequence and show that the sequence so constructed is related to Fibonacci numbers.

DEFINITION 4.1. Let k be a given positive integer. A set of integers is said to be a P_k set if every pair of distinct elements in the set have the property p_k. A sequence of integers is said to be a $P_{r,k}$ sequence if every r consecutive terms of the sequence constitute a P_k set.

Given a positive integer k, we can always find two integers α,β having the property p_k. Conversely, given two integers α,β, we can always find a positive integer k such that α,β have the property p_k. If S is a given P_k set and j is a given integer, then by multiplying all the elements of S by j, we obtain a P_{kj^2} set.

Suppose we are given two numbers $a_1 < a_2$ with property p_k and we want to extend the set $\{a_1,a_2\}$ such that the resulting set is also a P_k set. Towards this end, in the next section we construct a $P_{3,k}$ sequence $\{a_n\}$.

2. CONSTRUCTION OF A $P_{3,k}$ SEQUENCE

Suppose

$$a_1 a_2 + k = b_1^2 \tag{1}$$

and let $a_3 \varepsilon \{a_1, a_2, \ldots\}$, a P_k set. Then we have

$$a_1 a_3 + k = x^2, \tag{2}$$

$$a_2 a_3 + k = y^2 \tag{3}$$

for some integers x, y. Eliminating a_3 from (2) and (3), we get the Diophantine equation

$$X^2 - a_1 a_2 Y^2 = k a_2 (a_2 - a_1) \tag{4}$$

where $X = a_2 x$, $Y = y$. Using (1) in (4), we obtain the Diophantine equation

$$X^2 - (b_1^2 - k) Y^2 = k(a_2^2 - b_1^2 + k). \tag{5}$$

One can check that $X = a_2(a_1 + b_1)$, $Y = a_2 + b_1$, is always a solution of (5). When $b_1^2 - k$ is positive and square-free, (5) is Pell's equation and so has an infinite number of solutions.

Henceforth we concentrate on the solution $X = a_2(a_1 + b_1)$, $Y = a_2 + b_1$ of (5). This gives

$$a_2 a_3 + k = b_2^2,$$

$$a_1 a_3 + k = c_1^2$$

with

$$b_2 = a_2 + b_1,$$

$$c_1 = a_1 + b_1,$$

$$a_3 = b_2 + c_1.$$

In what follows, we construct three sequences $\{a_n\}$, $\{b_n\}$, $\{c_n\}$ where $a_1, a_2, a_3, b_1, b_2, c_1$ are as above. We say that $\{b_n\}$ and $\{c_n\}$ are the sequences associated with $\{a_n\}$. Taking

$$b_3 = a_3 + b_2,$$
$$c_2 = a_2 + b_2,$$
$$a_4 = b_3 + c_2,$$

we have

$$2(a_3+a_2)-a_1 = 2a_3+2a_2-(c_1-b_1)$$
$$= 2a_3+2a_2-(a_3-b_2)+b_1 = a_3+a_2+(a_2+b_2)+b_1$$
$$= a_3+a_2+c_2+b_1 = a_3+c_2+b_2 = b_3+c_2 = a_4.$$

Using this fact we have

$$a_2a_4+k = 2a_2a_3+2a_2^2-a_1a_2+k$$
$$= 2(b_2^2-k)+2(b_2-b_1)^2-(b_1^2-k)+k = (2b_2-b_1)^2$$
$$= (b_2+a_2)^2 = c_2^2$$

and

$$a_3a_4+k = 2a_3^2+2a_2a_3-a_1a_3+k$$
$$= 2(b_2+c_1)^2+2(b_2^2-k)-(c_1^2-k)+k = (2b_2+c_1)^2$$
$$= (b_2+a_3)^2 = b_3^2.$$

For the construction of the sequences $\{a_n\}$, $\{b_n\}$ and $\{c_n\}$, the following diagram may be helpful :

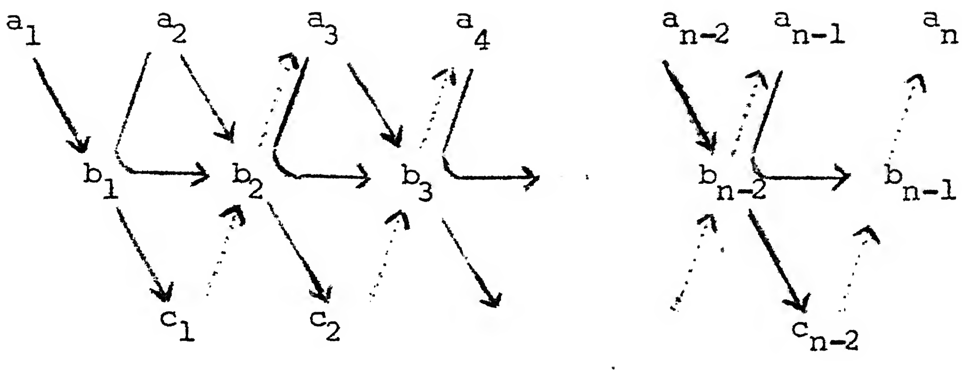

Diagram 1

Explanation for the diagram : Write $b_1 = \sqrt{a_1a_2+k}$ in the second row, in the space in between a_1 and a_2 and write $c_1 = \sqrt{a_1a_3+k}$ in the third row, in the space beneath a_2. Along the arrows shown by thick lines, sum the elements of the first and the second rows to get the elements of the third row ; along the curved arrows, sum the elements of the first and the second rows to get the elements of the second row ; along the arrows ...ed lines, sum the elements of the second and the ... get the elements of the first row. The discussion ...ling lines shows that the scheme provided by our ...alid for $a_1, a_2, a_3, a_4, b_1, b_2, b_3$ and c_1, c_2. Let $n > 2$. validity of the diagram for $a_1, \ldots, a_n, b_1, \ldots, b_{n-1}$ and

$c_1,\ldots,c_{n-2}$, it can be proved without much difficulty that

$$2(a_n+a_{n-1})-a_{n-2} = a_{n+1} \qquad (6)$$

and that the scheme is valid for $a_1,\ldots,a_{n+1},b_1,\ldots,b_n$ and $c_1,\ldots,c_{n-1}$.

3. PROPERTIES OF THE CONSTRUCTED SEQUENCES

THEOREM 4.1. The three sequences $\{a_n\}$, $\{b_n\}$ and $\{c_n\}$ have the same recurrence relation.

Proof. We have $a_{n+1} = 2(a_n+a_{n-1})-a_{n-2}$ (see (6)). Now

$$b_{n+1} = a_{n+1} + b_n = c_{n-1} + 2b_n = a_{n-1} + b_{n-1} + 2b_n$$
$$= 2b_n + b_{n-1} + (b_{n-1}-b_{n-2}).$$

i.e.,

$$b_{n+1} = 2(b_n+b_{n-1})-b_{n-2} \qquad (7)$$

and

$$c_{n+1} = a_{n+1} + b_{n+1} = 2a_{n+1} + b_n = 2(c_{n-1} + b_n) + b_n$$
$$= 2c_{n-1} + b_n + 2(c_n - a_n)$$
$$= 2(c_n + c_{n-1}) + (a_n + b_{n-1})-2a_n.$$

i.e.,

$$c_{n+1} = 2(c_n + c_{n-1}) - c_{n-2}. \qquad (8)$$

Hence the theorem is proved.

Now we obtain some more relations. First, using $a_{n+1} = c_{n+1} - b_{n+1}$ and $a_{n+2} = c_n + b_{n+1}$, we have

$$a_{n+1} + a_{n+2} = c_n + c_{n+1}.$$

i.e.,

$$a_{n+1} - c_n = -(a_{n+2} - c_{n+1}). \tag{9}$$

Next, from $b_n = c_n - a_n$ and $b_n = b_{n+1} - a_{n+1}$, we get

$$2b_n = (c_n + b_{n+1}) - a_{n+1} - a_n.$$

This yields

$$2b_n = a_{n+2} - a_{n+1} - a_n. \tag{10}$$

Next

$$\begin{aligned} a_{n+2} - a_{n+1} + a_n &= (b_{n+1} + c_n)-(b_{n+1} - b_n) + a_n \\ &= c_n + b_n + a_n . \end{aligned}$$

i.e.,

$$a_{n+2} - a_{n+1} + a_n = 2c_n. \tag{11}$$

From (10), we obtain $a_{n+2} = a_{n+1} + a_n + 2\sqrt{a_n a_{n+1} + k}$ and from (6), we have $a_{n+2} = 2(a_{n+1} + a_n) - a_{n-1}$. Hence we get

$$a_{n+1} + a_n - a_{n-1} = 2\sqrt{a_n a_{n+1} + k}.$$

This gives the relation

$$a_{n+1}^2 + a_n^2 + a_{n-1}^2 - 2a_{n-1}a_n - 2a_{n-1}a_{n+1} - 2a_n a_{n+1} = 4k. \tag{12}$$

Now we derive a relation for the Fibonacci sequence $\{F_n\}$ which is defined by

$$F_1 = F_2 = 1,$$
$$F_{n+2} = F_{n+1} + F_n.$$

V.E.Hoggatt,Jr. and G.E.Bergum [2] showed that any three terms of the Fibonacci sequence whose subscripts are consecutive even integers are such that the product of any two of them increased by 1 is a perfect square. This fact together with (12) leads to the relation

$$F_{2n}^2 + F_{2n+2}^2 + F_{2n+4}^2 - 2F_{2n}F_{2n+2} - 2F_{2n+2}F_{2n+4} - 2F_{2n}F_{2n+4} = 4. \qquad (13)$$

Next we shall exhibit a relationship between either of the sequences $\{a_n\}$, $\{b_n\}$, $\{c_n\}$ and the Fibonacci sequence $\{F_n\}$.

THEOREM 4.2.

$$a_n = -F_{n-3}F_{n-2}a_1+F_{n-3}F_{n-1}a_2+F_{n-2}F_{n-1}a_3, n \geq 4. \quad (14)$$

Proof. From (6), we get

$$a_4 = 2(a_3+a_2)-a_1 = -F_1F_2a_1+F_1F_3a_2+F_2F_3a_3,$$

$$a_5 = 2(a_4+a_3)-a_2 = -2a_1+3a_2+6a_3 = -F_2F_3a_1+F_2F_4a_2+F_3F_4a_3,$$

$$a_6 = 2(a_5+a_4)-a_3 = -6a_1+10a_2+15a_3 = -F_3F_4a_1+F_3F_5a_2+F_4F_5a_3.$$

So the theorem is true for n = 4,5,6. Let $n \geq 4$ and assume that the theorem is true for all integers j upto n. Using (6) we have

$$\begin{aligned} a_{n+1} &= 2(-F_{n-3}F_{n-2}a_1+F_{n-3}F_{n-1}a_2+F_{n-2}F_{n-1}a_3) \\ &\quad + 2(-F_{n-4}F_{n-3}a_1+F_{n-4}F_{n-2}a_2+F_{n-3}F_{n-2}a_3) \\ &\quad - (-F_{n-5}F_{n-4}a_1+F_{n-5}F_{n-3}a_2+F_{n-4}F_{n-3}a_3). \end{aligned}$$

i.e.,

$$a_{n+1} = (-2F_{n-3}F_{n-2}-2F_{n-4}F_{n-3}+F_{n-5}F_{n-4})a_1$$
$$+ (2F_{n-3}F_{n-1}+2F_{n-4}F_{n-2}-F_{n-5}F_{n-3})a_2$$
$$+ (2F_{n-2}F_{n-1}+2F_{n-3}F_{n-2}-F_{n-4}F_{n-3})a_3. \qquad (15)$$

The coefficient of a_1 in (15)

$$=-[2F_{n-3}(F_{n-2}+F_{n-4})-F_{n-4}(F_{n-3}-F_{n-4})]$$
$$=-(2F_{n-3}F_{n-2}+F_{n-3}F_{n-4}+F^2_{n-4})$$
$$= -(2F_{n-3}F_{n-2}+F_{n-4}F_{n-2}) = -F_{n-2}(2F_{n-3}+F_{n-4})$$
$$= - F_{n-2}(F_{n-3} + F_{n-2}) = -F_{n-2}F_{n-1}.$$

The coefficient of a_2 in (15)

$$= 2F_{n-3}F_{n-1} + 2F_{n-4}F_{n-2}-F_{n-5}F_{n-3}$$
$$= F_{n-3}(2F_{n-1}-F_{n-5})+2F_{n-4}F_{n-2}$$
$$= F_{n-3}(F_{n-1}+F_{n-2}+F_{n-4})+2F_{n-4}F_{n-2}$$
$$= F_{n-3}F_{n-1}+F_{n-2}(F_{n-3}+F_{n-4})+F_{n-4}(F_{n-3}+F_{n-2})$$
$$= F_{n-3}F_{n-1}+F^2_{n-2}+F_{n-4}F_{n-1} = F_{n-1}F_{n-2}+F^2_{n-2}=F_{n-2}F_n.$$

The coefficient of a_3 in (15)

$$= 2F_{n-2}F_{n-1}+2F_{n-3}F_{n-2}-F_{n-4}F_{n-3}$$
$$= 2F_{n-2}F_{n-1}+F_{n-3}(F_{n-2}+F_{n-3})$$
$$= 2F_{n-2}F_{n-1}+F_{n-3}F_{n-1}=F_{n-1}(2F_{n-2}+F_{n-3})=F_{n-1}(F_{n-2}+F_{n-1})$$
$$= F_{n-1}F_n.$$

This proves Theorem 4.2.

REMARK 4.1. The relations (6),(7) and (8) imply that (14) remains true if the a's are replaced by b's or by c's.

Now we express b's in terms of a_1, a_2, a_3. We have

$$2b_2 = -a_1+a_2+a_3.$$

Using $a_4 = 2(a_3+a_2)-a_1$, we obtain

$$2b_3 = -a_2+a_3+a_4 = -a_1+a_2+3a_3,$$

$$2b_4 = -a_2+a_3+3a_4 = -3a_1+5a_2+7a_3.$$

Suppose

$$2b_n = -r_n a_1+s_n a_2+t_n a_3.$$

Then

$$\begin{aligned} 2b_{n+1} &= -r_n a_2+s_n a_3+t_n a_4 \\ &= -t_n a_1+2(t_n-r_n)a_2+(2t_n+s_n)a_3. \end{aligned}$$

Hence

$$2b_{n+1} = -r_{n+1}a_1+s_{n+1}a_2+t_{n+1}a_3$$

where

$$\left.\begin{aligned} &t_2 = 1, t_3 = 3, t_4 = 7, \\ &r_{n+1} = t_n \\ &s_{n+1} = 2t_n-t_{n-1}, \\ &t_{n+1} = 2(t_n+t_{n-1})-t_{n-2} (n \geq 4). \end{aligned}\right\} \qquad (16)$$

Next we express c's in terms of a_1, a_2, a_3. We have

$$2c_1 = a_1-a_2+a_3.$$

Again using $a_4 = 2(a_3+a_2)-a_1$, we have

$$2c_2 = a_2-a_3+a_4 = -a_1+3a_2+a_3,$$

$$2c_3 = -a_2+3a_3+a_4 = -a_1+a_2+5a_3.$$

Suppose

$$2c_n = -u_n a_1+v_n a_2+w_n a_3.$$

Then

$$2c_{n+1} = -u_n a_2+v_n a_3+w_n a_4$$

$$= -w_n a_1+(2w_n-u_n)a_2+(2w_n+v_n)a_3.$$

Hence

$$2c_{n+1} = -u_{n+1}a_1+v_{n+1}a_2+w_{n+1}a_3$$

where

$$\left.\begin{aligned} &w_1 = 1, w_2 = 1, w_3 = 5,\\ &u_{n+1} = w_n\\ &v_{n+1} = 2w_n-w_{n-1},\\ &w_{n+1} = 2(w_n+w_{n-1})-w_{n-2} \quad (n \geq 3). \end{aligned}\right\} \qquad (17)$$

Thus the sequences $\{a_n\}$, $\{b_n\}$, $\{c_n\}$, $\{t_n\}$ and $\{w_n\}$ have the same recurrence relation.

Next we consider the possibility for the coincidence of the sequences $\{a_n\}$ and $\{c_n\}$. In this regard, we have the following

THEOREM 4.3. Let $\{a_n\}$ be a $P_{3,k}$ sequence with the associated sequences $\{b_n\}$ and $\{c_n\}$. The following statements are equivalent :

(i) $a_{n+1} = c_n$ for some integer $n \geq 1$

(ii) $a_{n+1} = c_n$ for all integers n

(iii) $b_{n+1} = b_n + c_n$,,

(iv) $c_{n+1} = b_{n+1} + c_n$,,

(v) $a_{n+1} = a_n + b_n$,,

(vi) $b_{n+2} = 3b_{n+1} - b_n$,,

(vii) $c_{n+2} = 3c_{n+1} - c_n$,,

(viii) $a_{n+2} = 3a_{n+1} - a_n$,,

(ix) $k = a^2_{n+1} - 3a_n a_{n+1} + a^2_n$,,

(x) $-k = b^2_{n+1} - 3b_n b_{n+1} + b^2_n$,,

(xi) $k = c^2_{n+1} - 3c_n c_{n+1} + c^2_n$,,

(xii) $a_n = -F_{2n-4}a_1 + F_{2n-2}a_2$

and

$b_n = -F_{2n-3}a_1 + F_{2n-1}a_2$

for all integers $n \geq 3$

(xiii) $\{b_n\}$ is a $P_{3,-k}$ sequence with the associated sequences $\{a_n\}$ and $\{b_n\}$ (where $b_n b_{n+1} - k = a^2_{n+1}$)

Proof. We adopt the following scheme : (i) ==> (ii) ==> (iii) ==> (iv) ==> (v) ==> (vi) ==> (vii) ==> (viii) ==> (ii) ==> (i) ; (v) ==> (ix) ==> (viii) ; (v) ==> (x) ==> (vi) ; (ii) ==> (xi) ==> (vii) ; (ii) ==> (xii) ==> (ii) and (x) ==> (xiii) ==> (x).

(i) ==> (ii). Follows from (9).

(ii) ==> (iii). Follows from $b_{n+1} = a_{n+1} + b_n$.

(iii) ==> (iv). Assume (iii) holds. Then

$$c_{n+1} = b_{n+2} - b_{n+1} = a_{n+2} = b_{n+1} + c_n.$$

Thus (iv) follows.

(iv) $\Longrightarrow$ (v). Assume (iv) holds. Then

$$a_{n+1} = b_n + c_{n-1} = c_n = a_n + b_n.$$

Thus (v) follows.

(v) $\Longrightarrow$ (vi). Assume (v) holds. Then

$$b_{n+2} = a_{n+2}+b_{n+1}=a_{n+1}+2b_{n+1}=(b_{n+1}-b_n)+2b_{n+1} = 3b_{n+1}-b_n.$$

Thus (vi) follows.

(vi) $\Longrightarrow$ (vii). Assume (vi) holds. Then

$$c_{n+1}+c_{n-1}=b_{n+1}+a_{n+1}+c_{n-1}=3b_n-b_{n-1}+a_{n+1}+c_{n-1}$$

$$= (a_{n+1}+b_n)+(b_n+c_{n-1})+b_n-b_{n-1}$$

$$= b_{n+1}+(a_{n+1}+b_n)-b_{n-1} = 2b_{n+1}-b_{n-1}$$

$$= 2(3b_n-b_{n-1})-b_{n-1} = 3(2b_n-b_{n-1})$$

$$= 3(b_n+a_n) = 3c_n.$$

Hence (vii) follows.

(vii) $\Longrightarrow$ (viii). Assume (vii) holds. Using $c_n=a_n+b_n$, we obtain

$$a_{n+2}+b_{n+2} = 3(a_{n+1}+b_{n+1})-(a_n+b_n).$$

i.e.,

$$2a_{n+2}+b_{n+1} = 3a_{n+1}+3b_{n+1}-a_n-b_n.$$

i.e.,

$$2a_{n+2} = 3a_{n+1}-a_n-b_n+2(a_{n+1}+b_n) = 5a_{n+1}-a_n-b_n.$$

Using (10) we get

$$4a_{n+2} = 10a_{n+1} - 2a_n + a_{n+2} - a_{n-1} - a_n.$$

i.e.,

$$a_{n+2} = 3a_{n+1} - a_n.$$

Hence (viii) follows.

(viii) $\Longrightarrow$ (ii). Assume (viii) holds. Then

$$a_{n+2} - a_{n+1} + a_n = 2a_{n+1}.$$

Using this in (11), we get $c_n = a_{n+1}$. Hence (ii) follows.

(ii) $\Longrightarrow$ (i). Clear.

(v) $\Longrightarrow$ (ix). Assume (v) holds. Then $b_n = a_{n+1} - a_n$. Using this in $a_n a_{n+1} + k = b_n^2$, we see the validity of (ix).

(ix) $\Longrightarrow$ (viii). Assume (ix) holds. Then

$$a_{n+1}a_{n+2} + k = (a_{n+2} - a_{n+1})^2$$

and

$$a_n a_{n+1} + k = (a_{n+1} - a_n)^2.$$

Hence

$$a_{n+1}(a_{n+2} - a_n) = (a_{n+2} - a_n)(a_{n+2} - 2a_{n+1} + a_n).$$

Since $a_n \neq a_{n+2}$, we get $a_{n+1} = a_{n+2} - 2a_{n+1} + a_n$. Hence (viii) follows.

(ii) $\Longrightarrow$ (x). Assume (ii) holds. Then (iii), (vi) and (ix) hold. Using $a_{n+1} = b_{n+1} - b_n$ in $k = a_{n+1}^2 - 3a_n a_{n+1} + a_n^2$, we obtain

$$k = (b_{n+1}-b_n)^2-3(b_n-b_{n-1})(b_{n+1}-b_n)+(b_n-b_{n-1})^2$$
$$= b_{n+1}^2+5b_n^2+b_{n-1}^2-5b_{n-1}b_n+3b_{n-1}b_{n+1}-5b_nb_{n+1}.$$

Using $b_{n-1} = 3b_n-b_{n+1}$, we obtain

$$-k = b_{n+1}^2-3b_nb_{n+1}+b_n^2.$$

Thus (x) follows.

(x) ==> (vi). Similar to (ix) ==> (viii).

(ii) ==> (xi). Assume (ii) holds. Since (ii) ==> (viii), we have

$$k = a_{n+2}^2-3a_{n+1}a_{n+2}+a_{n+1}^2 \quad = c_{n+1}^2-3c_nc_{n+1}+c_n^2.$$

Thus (xi) follows.

(xi) ==> (vii). Similar to (ix) ==> (viii).

(ii) ==> (xii). Assume (ii) holds. Then (v), (vi) and (viii) hold. From $a_{n+2} = 3a_{n+1}-a_n$, we have

$$a_3 = -a_1+3a_2 = -F_2a_1+F_4a_2,$$

$$a_4 = -a_2+3a_3 = -3a_1+8a_2 = -F_4a_1+F_6a_2.$$

Assume $a_j = -F_{2j-4}a_1 + F_{2j-2}a_2$ for all integers j upto n and $j \geq 3$. Then

$$a_{n+1} = 3a_n-a_{n-1} = 3(-F_{2n-4}a_1+F_{2n-2}a_2)-(-F_{2n-6}a_1+F_{2n-4}a_2)$$
$$= -(2F_{2n-4}+F_{2n-5})a_1+(2F_{2n-2}+F_{2n-3})a_2$$
$$= -(F_{2n-4}+F_{2n-3})a_1+(F_{2n-2}+F_{2n-1})a_2$$
$$= -F_{2n-2}a_1+F_{2n}a_2.$$

Next,

$$b_1 = -a_1 + a_2 = -F_{-1}a_1 + F_1 a_2,$$

$$b_2 = a_2 + b_1 = -a_1 + 2a_2 = -F_1 a_1 + F_3 a_2.$$

Assume $b_j = -F_{2j-3}a_1 + F_{2j-1}a_2$ for all integers j upto n and $j \geq 1$. Then

$$b_{n+1} = 3b_n - b_{n-1} = 3(-F_{2n-3}a_1 + F_{2n-1}a_2)$$
$$-(-F_{2n-5}a_1 + F_{2n-3}a_2)$$
$$= -(2F_{2n-3} + F_{2n-4})a_1 + (2F_{2n-1} + F_{2n-2})a_2$$
$$= -(F_{2n-3} + F_{2n-2})a_1 + (F_{2n-1} + F_{2n})a_2$$
$$= -F_{2n-1}a_1 + F_{2n+1}a_2.$$

Thus (xii) follows.

(xii) $\Longrightarrow$ (ii). Assume (xii) holds. Let $n \geq 1$. We have

$$c_n = a_{n+2} - b_{n+1} = (-F_{2n}a_1 + F_{2n+2}a_2)$$
$$-(-F_{2n-1}a_1 + F_{2n+1}a_2)$$
$$= -F_{2n-2}a_1 + F_{2n}a_2 = a_{n+1}.$$

Hence (ii) follows.

(x) $\Longrightarrow$ (xiii). Assume (x) holds. Then (vi) holds. So

$$b_n b_{n+1} - k = (b_{n+1} - b_n)^2 = a_{n+1}^2.$$

Next,

$$b_{n-1}b_{n+1} - k = b_{n-1}b_{n+1} + b_{n+1}^2 - 3b_n b_{n+1} + b_n^2.$$

Using $b_{n+1} = 3b_n - b_{n-1}$, we obtain

$$b_{n-1}b_{n+1}-k = b_n^2.$$

Thus (xiii) follows.

(xiii) ==> (x). Assume (xiii) holds. Then

$$k = b_n b_{n+1} - a_{n+1}^2 = b_n b_{n+1} - (b_{n+1}-b_n)^2.$$

This yields

$$-k = b_{n+1}^2 - 3b_n b_{n+1} + b_n^2.$$

Hence (x) follows. This completes the proof of Theorem 4.3.

4. F-TYPE $P_{3,k}$ SEQUENCES

DEFINITION 4.2. Let $\{a_n\}$ be a $P_{3,k}$ sequence together with the associated sequences $\{b_n\}$ and $\{c_n\}$. We say that $\{a_n\}$ is an F-type sequence if the sequence $\{a_1, b_1, a_2, b_2, a_3, b_3, \ldots,\}$, obtained by juxtaposing the two sequences $\{a_n\}$ and $\{b_n\}$, is of Fibonacci type. i.e., $f_1 = a_1, f_2 = b_1$ and $f_{n+2} = f_{n+1} + f_n$.

THEOREM 4.4. A $P_{3,k}$ sequence $\{a_n\}$ with the associated sequences $\{b_n\}$ and $\{c_n\}$ for which any one of the equivalent statements in Theorem 4.3. holds is an F-type sequence. Conversely, given a Fibonacci type sequence $T = \{g, h, g+h, g+2h, \ldots\}$ where g, h are two positive integers with $g < h$, if $\{a_n\}$ and $\{b_n\}$ are the sequences formed by taking the terms in the odd and even places respectively of T, in the same order

as they appear in T, then there is an integer k such that $\{a_n\}$ is an F-type $P_{3,k}$ sequence for which the equivalent statements in Theorem 4.3. hold.

Proof. (==>). Using $c_{n-1} = a_{n-1} + b_{n-1}$, we get $a_n = a_{n-1} + b_{n-1}$ for $n \geq 2$. Already we have $b_n = a_{n-1} + b_{n-1}$ for $n \geq 2$, Hence the sequence $\{a_1, b_1, a_2, b_2, \ldots\}$ is of Fibonacci type.

(<==) we have

$$\left.\begin{aligned} &a_1 = g, b_1 = h, \\ &a_n = F_{2n-3}g+F_{2n-2}h, b_n = F_{2n-2}g+F_{2n-1}h, n \geq 2 \end{aligned}\right\} \qquad (18)$$

where $\{F_n\}$ is the Fibonacci sequence. One can check that

$$a_n + a_{n+2} = 3a_{n+1} \text{ for all } n \geq 1. \qquad (19)$$

Now

$$(a_{n+2}^2 - 3a_{n+1}a_{n+2} + a_{n+1}^2) - (a_{n+1}^2 - 3a_n a_{n+1} + a_n^2)$$
$$= (a_{n+2}^2 - a_n^2) - 3a_{n+1}(a_{n+2} - a_n)$$
$$= (a_{n+2} - a_n)(a_{n+2} + a_n - 3a_{n+1}) = 0 \text{ for all } n \geq 1.$$

Hence we have

$$a_{n+1}^2 - 3a_n a_{n+1} + a_n^2 = a_{n+2}^2 - 3a_{n+1}a_{n+2} + a_{n+1}^2$$
$$= \text{constant, for all } n.$$

Let $a_{n+1}^2 - 3a_n a_{n+1} + a_n^2 = k$. In particular, putting $n = 1$, we get

$$k = h^2 - gh - g^2.$$

We have, using (20),

$$a_n a_{n+1}+k = (F_{2n-3}F_{2n-1}-1)g^2+(F_{2n-3}F_{2n}+F_{2n-2}F_{2n-1}-1)gh + (F_{2n-2}F_{2n}+1)h^2.$$

Now

$$F_{2n-3}F_{2n}-1 = (F_{2n-2} - F_{2n-4})(F_{2n-1} + F_{2n-2})-1$$
$$= F_{2n-2}F_{2n-1} + F_{2n-2}^2 - F_{2n-4}F_{2n-1} - F_{2n-3}^2$$
$$= F_{2n-2}F_{2n-1} + (F_{2n+2} + F_{2n-3})(F_{2n-2} - F_{2n-3}) - F_{2n-4}F_{2n-1}$$
$$= F_{2n-2}F_{2n-1}.$$

Hence

$$a_n a_{n+1}+k = F_{2n-2}^2 g^2 +2F_{2n-2}F_{2n-1}gh +F_{2n-1}^2h^2 = b_n^2 .$$

Next

$$a_{n-1}a_n+k = (F_{2n-5}F_{2n-1} - 1)g^2 + (F_{2n-5}F_{2n} + F_{2n-4}F_{2n-1} -1)gh + (F_{2n}F_{2n-4} + 1)h^2.$$

The coefficient of $g^2 = F_{2n-5}(F_{2n-2}+F_{2n-3}) - 1$

$$= F_{2n-5}(F_{2n-3} + F_{2n-4}) + F_{2n-5}F_{2n-3} - 1$$
$$= 2(F_{2n-4}^2 + 1) + F_{2n-5}F_{2n-4} - 1$$
$$= F_{2n-4}(F_{2n-4} + F_{2n-3}) + 1 = F_{2n-4}F_{2n-2} + 1 = F_{2n-3}^2.$$

The coefficient of $gh = F_{2n-5}(F_{2n-1} + F_{2n-2}) + F_{2n-4}F_{2n-1} - 1$

$$= F_{2n-1}(F_{2n-5} + F_{2n-4}) + F_{2n-5}F_{2n-2} - 1$$
$$= F_{2n-1}F_{2n-3} + F_{2n-5}F_{2n-2} - 1 = F_{2n-2}^2 + F_{2n-5}F_{2n-2}$$
$$= F_{2n-2}(F_{2n-2} + F_{2n-5}) = F_{2n-2}(F_{2n-3} + F_{2n-4} + F_{2n-5})$$
$$= 2F_{2n-2}F_{2n-3}.$$

The coefficient of $h^2 = (F_{2n-1} + F_{2n-2})F_{2n-4} + 1$

$= (F_{2n-2} + F_{2n-3})F_{2n-4} + F_{2n-2}F_{2n-4} + 1$

$= 2(F_{2n-3}^2 -1) + F_{2n-3}F_{2n-4} + 1$

$= F_{2n-3}(2F_{2n-3} + F_{2n-4}) -1 = F_{2n-3}(F_{2n-3} + F_{2n-2}) -1$

$= F_{2n-3}F_{2n-1} -1 = F_{2n-2}^2.$

Hence

$$a_{n-1}a_{n+1} + k = (F_{2n-3}g + F_{2n-2}h)^2 = a_n^2.$$

Consequently the sequence $\{a_n\}$ is an F-type $P_{3,k}$ sequence with the associated c-sequence given by $c_n = a_{n+1}$ for all integers $n \geq 1$.

5. THE DIOPHANTINE EQUATION $x^2-5y^2 = 4k$

THEOREM 4.5. Given a positive integer k, an F-type $P_{3,k}$ sequence exists if and only if the Diophantine equation

$$x^2-5y^2 = 4k \tag{21}$$

is solvable in integers.

Proof. (==>). Let $\{a_n\}$ be an F-type $P_{3,k}$ sequence with the associated sequence $\{b_n\}$ so that $\{a_1, b_1, a_2, b_2, \ldots\}$ is a sequence of Fibonacci type wherein the relations are given by (18). Then

$$k = h^2-gh-g^2.$$

i.e.,

$$h^2-gh-(g^2+k) = 0.$$

Treating this as a quadratic equation in h, we obtain

$$h = \frac{g \pm \sqrt{5g^2+4k}}{2} .$$

This implies

$$5g^2+4k = A^2$$

for some integer A. Hence the equation (21) is solvable in integers.

(<==). Let (x,y) be an integral solution of (21). Then $x \equiv y \pmod 2$. Form the Fibonacci type sequence $\{a_1, b_1, a_2, b_2, \ldots\}$ by taking $a_1 = y$, $b_1 = \frac{x+y}{2}$. Then by Theorem 4.4. there is an integer k' such that $\{a_n\}$ is an F-type $P_{3,k'}$ sequence. We have $k' = a_2^2-3a_1a_2+a_1^2$. Since $a_2 = a_1+b_1 = \frac{x+3y}{2}$, we obtain $k' = \frac{x^2-5y^2}{4} = k$.

THEOREM 4.6. Given a positive integer k, a necessary condition for the existence of an F-type $P_{3,k}$ sequence is that

$$k \not\equiv 2,3,6,7,8,10,12,13,14,17,18 \pmod{20}$$

and

$$k \not\equiv 10,15,35,40,60,65,85,90 \pmod{100}.$$

Proof. Assume that an F-type $P_{3,k}$ sequence exists. Then by Theorem 4.5., the equation (21) is solvable in integers. G.H.Hardy and E.M.Wright [1] showed that $k \not\equiv 2,3 \pmod 5$.

Now $k = h^2-gh-g^2$ where $g = y, h = \frac{x+y}{2}$. If g,h are both even, then $k \equiv 0 \pmod 4$. When g,h are both odd, if $h \equiv g \pmod 4$

then $k \equiv 3 \pmod 4$ and if $h \not\equiv g \pmod 4$, then $k \equiv 1 \pmod 4$. When h is odd, if $g \equiv 0 \pmod 4$, then $k \equiv 1 \pmod 4$ and if $g \equiv 2 \pmod 4$, then $k \equiv 3 \pmod 4$. When g is odd, if $h \equiv 0 \pmod 4$, then $k \equiv 3 \pmod 4$ and if $h \equiv 2 \pmod 4$, then $k \equiv 1 \pmod 4$. Thus $k \not\equiv 2 \pmod 4$. Consequently $k \not\equiv 2,3,6,7,8,10,12,13,14,17,18 \pmod{20}$.

Next, if $k \equiv 10,15,35,40,60,65,85,$ or $90 \pmod{100}$, write $k = 100k_1 + i$ where $i = 10,15,35,40,60,65,85$ or 90. Then (21) gives $x^2 - 5y^2 = 400k_1 + 4i$. Since $5 \mid i$, we have $5 \mid x$. Putting $x = 5x_1$, we obtain $5x_1^2 - y^2 = 80k_1 + i_1$ where $i_1 = 8,12,28,32,48,52,68,$ or 72. This implies $y^2 \equiv 2$ or $3 \pmod 5$, which is impossible. Hence $k \not\equiv 10,15,35,40,60,65,85,90 \pmod{100}$. This completes the proof of Theorem 4.6.

In the following theorem, we prove a result for the Diophantine equation (21) by considering the terms of the corresponding F-type $P_{3,k}$ sequence.

THEOREM 4.7. Given a positive integer k, the number of distinct classes of solutions of the equation (21) is divisible by 3.

Proof. If (21) is not solvable in integers, then the theorem trivially holds. Assume the solvability of (21). Let (x_1, y_1) be an integral solution of (21). Take $a_1 = y_1$, $b_1 = \frac{x_1+y_1}{2}$ and $a_2 = a_1 + b_1$. i.e., $a_2 = \frac{x_1+3y_1}{2}$. Then by Theorem 4.5., we have $k = a_2^2-3a_1a_2+a_1^2$ and $\{a_n\}$ is an

F-type $P_{3,k}$ sequence. We have

$$b_2 = a_2 + b_1 = x_1 + 2y_1,$$
$$a_3 = a_2 + b_2 = \frac{3x_1+7y_1}{2},$$
$$b_3 = a_3 + b_2 = \frac{5x_1+11y_1}{2},$$
$$a_4 = a_3 + b_3 = 4x_1 + 9y_1,$$
$$b_4 = a_4 + b_3 = \frac{13x_1+29y_1}{2}.$$

Choose x_i, y_i $(i = 2,3,4)$ such that $y_i = a_i$ and $\frac{x_i+y_i}{2} = b_i$. i.e., $x_i = 2b_i - y_i$. Then $x_2 = \frac{3x_1 + 5y_1}{2}$, $x_3 = \frac{7x_1+15y_1}{2}$, $x_4 = \frac{9x_1+20y_1}{2}$. One can easily check that $x_i + \sqrt{5}\, y_i$ $(i = 2,3,4)$ are solutions of (21). Since $\frac{x_1y_2-y_1x_2}{4k} = \frac{1}{2}$, $\frac{x_1y_3-y_1x_3}{4k} = \frac{3}{2}$ and $\frac{x_2y_3-y_2x_3}{4k} = \frac{1}{2}$, by Theorem 3.3. (page 100) it follows that each $x_i + \sqrt{5}\, y_i$ $(i = 1,2,3)$ belongs to a distinct class of solutions of (21). Now

$$x_4 + \sqrt{5}\, y_4 = (9x_1+20y_1) + \sqrt{5}\,(4x_1+9y_1)$$
$$= (x_1 + \sqrt{5}\, y_1)(9 + 4\sqrt{5})^n.$$

Since $9+4\sqrt{5}$ is the fundamental solution of the Pell's equation

$$A^2 - 5B^2 = 1,$$

it follows that $x_1 + \sqrt{5}\, y_1$ and $x_4 + \sqrt{5}\, y_4$ belong to the same class of solutions of (21). Thus, given a solution $x_1 + \sqrt{5}\, y_1$ of (21), we obtain three consecutive terms a_i $(i = 1,2,3)$ of an F-type $P_{3,k}$ sequence which in turn yield two more solutions $x_i + \sqrt{5}\, y_i$ $(i = 2,3)$ of (21) such that

$x_i + \sqrt{5}\, y_i$ $(i = 1,2,3)$ belong to different classes of solutions of (21). Further, it follows by a simple induction that, for any integers i, i', j, the terms a_{3i+j} and $a_{3i'+j}$ $(j = 0,1,2)$ yield solutions of (21) which belong to the same class. Hence every F-type $P_{3,k}$ sequence contributes exactly 3 distinct classes of solutions of (21). Consequently the number of distinct classes of solutions of (21) is divisible by 3.

REMARK 4.2. When k is square-free, B.Stolt [4] proposed a proof for the result that the number of distinct classes of solutions of the Diophantine equation

$$U^2 - DV^2 = 4k \text{ (D: positive, square-free)}$$

is a power of 2. The invalidity of his statement is established by our Theorem 4.7.

DEFINITION 4.3. Given a positive integer k, two $P_{3,k}$ sequences $\{a_n\}$ and $\{a'_n\}$ are said to be distinct if there do not exist integers r and s such that

$$a_r = a'_s .$$

THEOREM 4.8. Given a positive integer k, the number of distinct F-type $P_{3,k}$ sequences is equal to $\frac{1}{3}$ of the number of distinct classes of solutions of (21).

Proof. Follows from Theorem 4.7.

6. THE DIOPHANTINE EQUATION $X^2+33Y^2 = Z^2$

We now determine those F-type $P_{3,k}$ sequences $\{a_n\}$ in which a_1 and a_4 also share the property p_k.

Suppose a_1 and a_4 share the property p_k. Then

$$a_1a_4 + k = \lambda^2$$

for some integer λ. Using $a_4 = -3a_1 + 8a_2$ and $k = a_2^2-3a_1a_2+a_1^2$, we have

$$a_2^2 + 5a_1a_2-2a_1^2 = \lambda^2.$$

This equation can be rewritten as

$$(2\lambda)^2 + 33a_1^2 = (5a_1+2a_2)^2.$$

Putting $X = 2\lambda$, $Y = a_1$, $Z = 5a_1 + 2a_2$, we obtain the Diophantine equation

$$X^2 + 33Y^2 = Z^2. \qquad (22)$$

Now we have to find the integer solutions of (22). Without loss of generality, we can assume that $\gcd(X,Y,Z) = 1$. Then $\gcd(X,Y) = \gcd(Y,Z) = \gcd(Z,X) = 1$. So at least two of X,Y,Z must be odd. If X and Y are both odd, then (22) implies that $Z^2 \equiv 2 \pmod 4$, which is impossible. Consequently one of X,Y is even and the other one is odd. In any case Z is odd.

Case (i). X is even and Y is odd. In this case $Z+X$ and $Z-X$ are both odd. If p is a prime number such that $p \mid Z+X$

and $p \mid Z-X$, then $p \mid 2Z$ and $p \mid 2X$. Since p is odd, we have $p \mid Z$ and $p \mid X$. This contradicts our assumption that $\gcd(Z,X) = 1$. Hence $\gcd(Z+X, Z-X) = 1$. Consequently, rewriting (22) as

$$(Z+X)(Z-X) = 33Y^2,$$

we see that there exist integers d_1, d_2, α, β such that

$$Z + X = d_1\alpha^2,$$
$$Z - X = d_2\beta^2$$

with $d_1d_2 = 33$ and $\gcd(\alpha,\beta) = 1$. Hence

$$X = \frac{d_1\alpha^2 - d_2\beta^2}{2},$$

$$Y = \alpha\beta,$$

$$Z = \frac{d_1\alpha^2 + d_2\beta^2}{2}$$

Case (ii). X is odd and Y is even. Now z+X and Z-X are even. Hence $\frac{Z+X}{2}$ and $\frac{Z-X}{2}$ are integers. We rewrite (22) as

$$\frac{Z+X}{2}\,\frac{Z-X}{2} = 33Y^2.$$

Since $\gcd(\frac{Z+X}{2}, \frac{Z-X}{2}) = 1$, there exist integers d_1, d_2, α, β such that

$$\frac{Z+X}{2} = d_1\alpha^2,$$

$$\frac{Z-X}{2} = d_2\beta^2$$

with $d_1d_2 = 33$ and $\gcd(\alpha,\beta) = 1$. So

$$X = d_1\alpha^2 - d_2\beta^2,$$

$$Y = 2\alpha\beta,$$

$$Z = d_1\alpha^2 + d_2\beta^2.$$

Having known a solution (X,Y,Z) of (22), we can find a_1 and a_2 using

$$a_1 = Y,\ a_2 = \frac{Z-5Y}{2}.$$

Then $k = a_2^2 - 3a_1a_2 + a_1^2$. In Case (i), $\frac{Z-5Y}{2}$ is an integer. In Case (ii), $2 \nmid Z-5Y$. Hence, in Case (ii), we take $a_1 = 2Y$, $a_2 = Z-5Y$ and $k = a_2^2 - 3a_1a_2 + a_1^2$.

Some F-type $P_{3,k}$ sequences $\{a_n\}$ in which a_1 and a_4 also share the property p_k are given in the following table.

k	a_1	a_2	a_3	a_4
19	1	6	17	45
139	2	15	43	114
145	8	27	73	192
1305	24	81	219	576
3895	3	67	198	527
10121	8	113	331	880
38475	45	270	765	2025
41305	24	241	699	1856

Table 1

7. $P_{r,k}$ SEQUENCES WITH $r \geq 4$

Our next investigation is on $P_{r,k}$ sequences with $r \geq 4$. As regards this, we prove the following

THEOREM 4.9. If $k \equiv 2 \pmod 4$, then there is no $P_{r,k}$ sequence with $r \geq 4$.

Proof. We follow the reasoning given by S.P.Mohanty [3]. Let $k \equiv 2 \pmod 4$ and let $\{a_n\}$ be a $P_{4,k}$ sequence. Then, for any two integers i, j satisfying $|j-i| \leq 3$, we have

$$a_i \cdot a_j + k = B^2 \qquad (23)$$

for some integer B. If $a_i \equiv 0 \pmod 4$ or if $a_j \equiv 0 \pmod 4$, then (23) implies $B^2 \equiv 2 \pmod 4$, which is impossible. Hence neither of a_i, a_j is $0 \pmod 4$. If $a_i \equiv a_j \pmod 4$, then (23) implies $B^2 \equiv 2$ or $3 \pmod 4$, a contradiction. So $a_i \not\equiv a_j \pmod 4$. Consequently the elements $a_i, a_{i+1}, a_{i+2}, a_{i+3}$ do not share the property p_k.

REFERENCES

1. G.H.Hardy and E.M.Wright, An Introduction to the Theory of Numbers, Oxford University Press, Third Edition, 1954. MR 16,673.

2. V.E.Hoggatt, Jr., and G.E.Bergum, A problem of Fermat and the Fibonacci sequence, Fibonacci Quart., 15(1977), 323-330. MR 56 # 15547.

3. S.P.Mohanty, On S(p)m sets (unpublished) (Communicated).

4. B.Stolt, On the Diophantine equations $u^2-Dv^2 = \pm 4N$, III, Ark. Mat., 3(1958), 117-132. MR 16,903.

CHAPTER 5

ON THE NUMBER OF COPRIME INTEGRAL SOLUTIONS OF $y^2=x^3+k$ AND SOME RELATED PROBLEMS

1. INTRODUCTION

The Diophantine equation $y^2=x^3+k$ has played a fundamental role in the development of number theory (see L.J. Mordell [5]). This equation is now known as Mordell's equation. For a complete bibliography for this equation one can see S.P. Mohanty [2].

Let $N'(k)$ denote the number of coprime integral solutions x,y of $y^2=x^3+k$. Mohanty [3] has proved that $\limsup_{k \to \infty} N'(k) \geq 6$ by showing that the equation $y^2= x^3+(t^6-6t^3+1)$ has six solutions $x,y \in Z[t]$ where Z denotes the ring of integers. They are $\pm P_i$, $i = 1,2,3$ where $P_i = (x,y)$ and $-P_i=(x,-y)$ and

$$P_1: x = 2, \qquad y = t^3-3$$
$$P_2: x = 2t, \qquad y = t^3+1$$
$$P_3: x = 2t^2, \qquad y = 3t^3-1$$

(For each integer t, each pair x,y is coprime).

Stephens [6] has proved that $\limsup_{k \to \infty} N'(k) \geq 8$ by showing that the above equation $y^2=x^3+(t^6-6t^3+1)$ has eight solutions $x,y \in Z[t]$. He has

$$P_4: \ x = t^4+2t^3+3t^2-1, y = -(t^6+3t^5+6t^4+4t^3-3t).$$

He has also shown that $\limsup_{k \to -\infty} N'(k) \geq 12$.

Mohanty's k was a polynomial of degree six. But there are polynomials of degree 4 for which the above results hold. We have

$$(2t^2+1)^2-(-2t)^3 = (2t^2+2t)^2-(-1)^3 = (2t^2+4t+3)^2 - (2t+2)^3$$

$= 4t^4+8t^3+4t^2+1$ whence $\limsup_{k \to \infty} N'(k) \geq 6$. Again

$$(3t^2+3t+3)^2-(2t+2)^3 = (3t^2-9t+3)^2 - (-4t+2)^3$$

$$= (3t^2+3t-1)^2-(2t)^3$$

$$= (27t^6+81t^5+108t^4+63t^3+9t^2-6t)^2$$

$$- (9t^4+18t^3+15t^2+2t-1)^3$$

$$= 9t^4+10t^3+3t^2-6t+1.$$

So the equation $y^2 = x^3+(9t^4+10t^3+3t^2-6t+1)$ has 8 coprime solutions (x,y) for $\gcd(t+1,3)=1$ and we have another proof of $\limsup_{k \to \infty} N'(k) \geq 8$. In the next section we improve this bound.

2. THE DIOPHANTINE EQUATION $y^2=x^3+k$

THEOREM 5.1. $\limsup_{k \to \infty} N'(k) \geq 12$.

Proof. Mohanty [4] has proved that $y^2 = x^3+ (16t^6+1)$ has three consecutive integer solutions for y by showing that

$$(4t^3+1)^2-(2t)^3 = (4t^3)^2-(-1)^3 = (4t^3-1)^2-(-2t)^3 = 16t^6+1.$$

This again proves that $\limsup_{k \to \infty} N'(k) \geq 6$. We list down the six solutions.

P_1 : $x = 2t$, $y = 4t^3+1$

P_2 : $x = -1$, $y = 4t^3$

P_3 : $x = -2t$, $y = 4t^3-1$

and $-P_1, -P_2, -P_3$ where $-P_i = (x,-y)$.

We can consider $y^2 = x^3 + (16t^6+1)$ as an elliptic curve E over the function field $Q(t)$ (Q is the field of rational numbers) on which there is an additive law. If (x_1,y_1) and (x_2,y_2) are two distinct points on E, their sum (x',y') is given by

$$x' = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2,$$

$$-y' = \left(\frac{y_2-y_1}{x_2-x_1}\right)(x'-x_1) + y_1.$$

Now we consider the x,y coordinates for $P_i \pm P_j$, $1 \le i < j \le 3$. We find that only three out of these six points namely,

P_1-P_2 : $x = 16t^4-16t^3+12t^2-6t+2$,

$y = -(64t^6-96t^5+96t^4-68t^3+36t^2-12t+3)$

P_1-P_3 : $x = 4t^4$, $y = -(8t^6+1)$

and P_2-P_3 : $x = 16t^4+16t^3+12t^2+6t+2$,

$y = -(64t^6+96t^5+96t^4+68t^3+36t^2+12t+3)$

have integral coordinates x,y if t is an integer.

To check that in a solution (x,y), the coordinates are coprime for all integers t, Euclid's algorithm may be applied.

For example, for P_1-P_2 we have

$$\gcd(16t^4-16t^3+12t^2-6t+2,\ 64t^6-96t^5+96t^4-68t^3+36t^2-12t+3)$$

$$= \gcd(8t^4-8t^3+6t^2-3t+1,\ 4t^3-4t^2+2t-1)$$

$$= \gcd(2t^2-t+1, 4t^3-4t^2+2t-1) = \gcd(2t^2-t+1, t) = \gcd(1,t) = 1.$$

Hence, there are atleast 12 distinct coprime solutions for $y^2 = x^3 + (16t^6+1)$ given by

P_1 : $x = 2t$, $y = 4t^3+1$

P_2 : $x = -1$, $y = 4t^3$

P_3 : $x = -2t$, $y = 4t^3-1$

P_4 : $x = 16t^4-16t^3+12t^2-6t+2$,

$y = 64t^6-96t^5+96t^4-68t^3+36t^2-12t+3$

P_5 : $x = 4t^4$, $y = 8t^6+1$

P_6 : $x = 16t^4+16t^3+12t^2+6t+2$,

$y = 64t^6+96t^5+96t^4+68t^3+36t^2+12t+3$

and $-P_1, -P_2, \ldots, -P_6$ where $-P_i = (x,-y)$ when $P_i = (x,y)$.

Thus $\limsup_{k \to \infty} N'(k) \geq 12$.

We pose below the following interesting problem:

Does there exist a polynomial $k(t)$ with integral coefficients and degree 4 such that $y(t)^2 = x(t)^3 + k(t)$ has atleast 12 solutions?

REMARKS: We have considered the equation $y(t)^2 = x(t)^3 + k(t)$, where $x(t)$, $y(t)$ and $k(t)$ are polynomials with integral coefficients. Using $k(t) = 4t^4+8t^3+4t^2+1$, we get

$17 = 3^2-(-2)^3 = 4^2 - (-1)^3 = 9^2 - 4^3$. $k(t) = t^6-6t^3+1$, t even, yields $17 = 5^2-2^3 = 9^2-4^3 = 23^2-8^3 = 282^2 - 43^3$. From $k(t) = 9t^4 + 10t^3 + 3t^2 - 6t + 1$, $\gcd(t+1, 3) = 1$, we obtain $17 = 9^2-4^3 = 3^2-(-2)^3 = 5^2-2^3 = 282^2 - 43^3$. Again from $k(t) = 16t^6+1$, we have $17 = 5^2-2^3 = 4^2-(-1)^3 = 3^2-(-2)^3 = 9^2 - 4^3 = 23^2-8^3 = 375^2-52^3$. We still miss the solution

$$378661^2-5234^3 = 17.$$

We would like to see a $k(t) = y(t)^2-x(t)^3$ which would yield the missing solution along with some other solution.

It is pointed out in [3] that it appears likely that $\limsup_{k \to \infty} N'(k) \neq \infty$. From earlier papers we had $\limsup_{k \to \infty} N'(k) \geq 8$. In this chapter we have shown that $\limsup_{k \to \infty} N'(k) \geq 12$.

If we look at the Lal, Jones and Blundon table (see also [1]) we find isolated examples with much larger values of $N'(k)$. For example $N'(17) = 16$, $N'(2089) \geq 28$, $N'(4481) \geq 24$, $N'(7057) \geq 22$ and $N'(1025) \geq 32$. Then one would be tempted to see a value of n bigger than what we have. However, we strongly feel that it will be a challenging problem even to show $n = 10$.

3. THE DIOPHANTINE EQUATION $by^2 = ax^3+k$

Denoting the number of coprime integer solutions of $y^2 = ax^3 + k$ by $N'(a,k)$, Jingcheng Tong [7] proved that $\limsup_{k \to \infty} N'(a,k) \geq 6$ holds for odd integer a and raised the following

PROBLEM. Does $\limsup_{k \to \infty} N'(a,k) \geq 6$ hold for even integer a?

We prove below that the answer to his question is in the affirmative. In fact we prove the result for the more general Diophantine equation $by^2=ax^3+k$ where a and b are any given non-zero integers.

Consider the following polynomials:

$$x_1 = 2bt, \qquad y_1 = 4ab^2t^3 + 1$$
$$x_2 = -2bt, \qquad y_2 = 4ab^2t^3 - 1$$
$$x_3 = 4ab^3t^4, \qquad y^3 = 8a^2b^4t^6 + 1$$

It is easy to check that $(x_i, \pm y_i)$ $(i=1,2,3)$ are solutions of the equation $by^2=ax^3+k$, where $k = 16a^2b^5t^6 + b$. By applying Euclid's algorithm, one can see that $\gcd(x_i,y_i)=1$, $i=1,2,3$. Hence if we denote the number of coprime integer solutions of the equation $by^2 = ax^3+k$ by $N'(a,b,k)$, then we have

THEOREM 5.2. $\limsup_{k \to \infty} N'(a,b,k) \geq 6$ holds for any given non-zero integers a and b.

By taking b=1 in Theorem 5.2, we obtain an affirmative answer for Tong's problem.

Next we prove a stronger result for a=4 and b=1. Consider the following polynomials:

$$x_1 = t, \qquad y_1 = 2t^3 + 1$$
$$x_2 = -t, \qquad y_2 = 2t^3 - 1$$
$$x_3 = -t^2, \qquad y_3 = 1$$
$$x_4 = t^4, \qquad y_4 = 2t^6+1$$

Without much difficulty, one can check that $(x_i, \pm y_i)$ $(i=1,2,3,4)$ are coprime integer solutions of the Diophantine equation $y^2 = 4x^3+k$, where $k = 4t^6+1$. Hence we have in Tong's notation,

THEOREM 5.3. $\limsup_{k \to \infty} N'(4,k) \geq 8$.

It would be an interesting problem to determine the integers $a \neq 0,1,4$ for which $\limsup_{k \to \infty} N'(a,k) \geq 8$ holds in Tong's notation.

REFERENCES

1. M. Lal, M.F. Jones and W.J. Blundon, Numerical solutions of the Diophantine equation $y^3-x^2 = k$, Math. Comp., 20 (1966), 322-325. MR 33 # 98.
2. S.P. Mohanty, On the Diophantine equation $y^2-k = x^3$, Ph.D. Diss., UCLA (1971).
3. ______________, A note on Mordell's equation $y^2= x^3+k$, Proc. Amer. Math. Soc., 39 (1973), 645-646. MR 47 # 4924.
4. ______________, On consecutive integer solutions for $y^2-k = x^3$, Proc. Amer. Math. Soc., 48 (1975), 281-285. MR 50 # 9787.
5. L.J. Mordell, Diophantine Equations, Pure and Appl. Math., Vol. 30, Academic Press, London and New York, 1969. MR 40 # 2600.

6. N.M. Stephens, On the number of coprime solutions of $y^2 = x^3 + k$, Proc. Amer. Math. Soc., 48 (1975), 325-327. MR 50 # 9788.

7. Jingcheng Tong, A note on the number of coprime integer solutions of $y^2 = ax^3 + k$, Indian J. Pure Appl. Math., 12 (1981), 1078-1079. Zbl. 469. 10006.

PUBLICATIONS

(a) The following papers, containing some of the results of the present thesis, have been accepted for publication :

1. On the number of coprime integral solutions of $y^2 = x^3+k$, J.Number Theory (Accepted in December, 1981).

2. The simultaneous Diophantine equations $5Y^2-20 = X^2$ and $2Y^2+1 = Z^2$, J.Number Theory (Accepted in September, 1982).

3. The simultaneous Diophantine equations $x^2+x+1 = 3z$, $y^2+y+1 = 3z^2$ and a generalization of a theorem of A.Brauer, Indian J. Pure Appl.Math. (Accepted in September, 1982).

(b) Revised version of the paper 'On the positive integral solutions of the Diophantine equation $x^3+by+1-xyz = 0$ $(b > 0)$' has been communicated to Bull.Malaysian Math.Soc.